# Schulen ans Netz - mit Sicherheit

„Wir sind schon drin“. Das sagen heute bereits viele niedersächsische Schulen. Beim Gang ins Internet ergeben sich neben vielen handwerklichen Problemen auch Fragen zum sicheren Umgang mit dem weltweiten Web. Ausführliche Hinweise und Empfehlungen für Schulleitungen, Lehrerinnen und Lehrer, Schülerinnen und Schüler sowie Eltern sind in der Broschüre **„Schulen ans Netz - mit Sicherheit“** zusammengefasst. Sie will die nötige Sensibilität für Sicherheits- und Datenschutzprobleme vermitteln, praktische Lösungen für weitere Fragestellungen vorstellen und soll helfen, mit den Herausforderungen des Internet konstruktiv und sachgerecht umzugehen.

# FAQ - Schulen ans Netz

Kurze Antworten auf die mir am häufigsten gestellten Fragen (FAQ) zu diesem Themenkomplex finden Sie hier:

**Welche Gefahren sind mit dem Internet verbunden?**

Die Gefahren und Risiken im Internet sind erheblich. Beim Surfen, beim Spielen und auch beim Austauschen von Nachrichten werden Datenspuren hinterlassen. Die Rechner und Übertragungswege im weltweiten Internet sind nicht kontrollierbar. Welchen Weg eine Nachricht nimmt oder in welchem Vermittlungsrechner die Nachricht bearbeitet wird, ist nicht transparent. Risiken für Vertraulichkeit, Integrität und Zurechenbarkeit personenbezogener Daten werden im Internet nicht hinreichend abgesichert. Ohne besondere Schutzmaßnahmen, die der Nutzer selbst treffen muss, kann sich ein Angreifer oft mit wenig Aufwand unerlaubten Zugang zu fremden Rechnern verschaffen und dort Daten ausspähen oder sogar manipulieren und zerstören.

**Welche Internetdienste sind in der Schule erlaubt?**

Das Internet besteht nicht nur aus dem „world wide web“ (www), das durch seinen multimediafähigen Mechanismus einfach zu bedienen und vielfach nutzbar ist. Die elektronische Post (E-Mail) und Usenet-News sind die meistgenutzten Dienste im Internet, Telnet ermöglicht den Zugang auf den Rechner von beliebigen Adressen aus, FTP dient dem Austausch großer Datenmengen, der „Domain Name Service“ (DNS) übersetzt den Rechnernamen in Internetadressen (IP) und mit dem „Simple Network Management Protocol“ (SNMP) können Netzwerkkomponenten von zentraler Stelle aus verwaltet werden. Welche dieser Dienste erforderlich und für die Nutzung freigegeben werden sollen, entscheidet die Schulleitung. Im Rahmen des Unterrichts können alle schulintern erlaubten Internetdienste benutzt werden. Maßgeblich sind im konkreten Fall die Anweisungen der unterrichtenden Lehrkraft, die für die Schüler/innen verbindlich sind.

**Wer trägt die Verantwortung für den Internetzugang der Schule?**

Grundsätzlich trägt die Schulleitung, die den Zugang zum Internet eröffnet, die Verantwortung für den Internetzugang der Schule. Jede Schule sollte verbindliche Regeln festlegen, damit alle Beteiligten wissen, wer das Internet in der Schule wann und wie nutzen darf, welche Kontrollen und welche Sanktionen vorgesehen sind.

**Wo ist nachlesbar, was erlaubt ist?**

Jede Schule sollte eine auf ihre Verhältnisse und Erfordernisse zugeschnittene Nutzungsordnung erstellen und bekannt machen, die zumindest folgende Festlegungen treffen sollte:

- die Verantwortlichkeiten des Internet-Auftritts der Schule,
- die Rechte und Pflichten des Systemadministrators und des Webmasters,
- die zugelassenen Internet-Dienste sowie die Rechte der einzelnen Nutzer,
- die Aufsichtspflicht der unterrichtenden Lehrer/innen und

- die Pflichten der Nutzer sowie Sanktionen bei Pflichtverletzungen.

**Was ist eine schuleigene Homepage?**

Mit einer eigenen Homepage haben Schulen die Möglichkeit sich im Netz zu präsentieren und Informationen über die Schule jedermann zur Verfügung zu stellen. Dies stellt eine weltweite Veröffentlichung von Informationen dar, die von jeder Person mit Internetanschluss aufgerufen und auf den eigenen Rechner heruntergeladen, verändert und genutzt werden können. Homepages erfüllen nicht nur einen Informationszweck, sondern bieten sich auch für eine direkte Kommunikation mit Schülerinnen und Schülern, Eltern und Freunden der Schule an. Die Verantwortung liegt grundsätzlich bei der Schulleitung oder der von ihr autorisierten Lehrkraft. Bei einer solchen Nutzung sollte deutlich gemacht werden, dass keine Gewähr für die Richtigkeit der angebotenen Informationen übernommen werden kann. Strafrechtlich relevante Meinungsäußerungen dürfen nicht zugelassen werden.

**Darf auf der Homepage alles veröffentlicht werden?**

Nein, in jedem Falle muss überprüft werden, ob die Veröffentlichung personenbezogener Daten auf der Homepage nach den datenschutzrechtlichen Bestimmungen des Schulrechtes und des Niedersächsischen Datenschutzgesetzes zulässig ist. Eine Veröffentlichung personenbezogener Daten von Lehrer/innen ist zulässig, sofern dies zur Kontaktaufnahme und –pflege erforderlich ist. Private Daten von Lehrkräften dürfen nur mit ausdrücklich erklärter Einwilligung veröffentlicht werden. Personenbezogene Daten von Schüler/innen und Erziehungsberechtigten dürfen grundsätzlich nur mit deren Einwilligung *(§ 4 NDSG)* auf der Homepage veröffentlicht werden.

**Wie steht es um ‚Gästebuch' und ‚Schwarzes Brett'?**

Homepages erfüllen nicht nur einen Informationszweck, sondern bieten sich auch für eine direkte Kommunikation an. Bei einer solchen Nutzung sollte deutlich gemacht werden, dass keine Gewähr für die Richtigkeit der zu findenden Angaben übernommen werden kann. Strafrechtlich relevante Meinungsäußerungen werden nicht zugelassen.

**Dürfen Schüler/innen selbständig Beiträge auf den Internetseiten der Schule veröffentlichen?**

Da die Schulleitung oder die von ihr beauftragte Lehrkraft für die Homepage verantwortlich ist, ist eine vorherige Genehmigung des Verantwortlichen erforderlich. Eine Ausnahme stellt die Veröffentlichung der Schülerzeitung auf der Homepage dar. Da die Redaktion der Schülerzeitung die Verantwortung für deren Inhalt trägt, wäre es denkbar, die Schülerzeitung auf einer eigenen Homepage mit eigenem Domainnamen auf dem Schulserver zu veröffentlichen.

**Dürfen Webcam-Aufnahmen ins Internet gestellt werden?**

Dieses wäre nur zulässig, wenn die Kameras so aufgestellt sind, dass die Bilder keine Daten mit Personenbezug enthalten. In Frage kommen daher allenfalls Übersichtsaufnahmen, die die Herstellung eines Personenbezuges definitiv ausschließen.

**Haben die Schüler/innen ein Recht auf vertrauliche Kommunikation?**

Im Unterricht nehmen Lehrer/innen Einsicht in die E-Mail-Kommunikation der Schüler/innen; denn der Unterricht liegt in der Verantwortung der Lehrkraft. Es besteht jedoch weder eine flächendeckende Überwachungspflicht noch ein generelles Überwachungsrecht.

**Dürfen Schüler/innen z. B. Nazi- oder Pornoseiten auf dem Schulcomputer aufrufen?**

Die Schule kann die Zugriffsmöglichkeiten festlegen. Zur Sicherung von Zugriffsbeschränkungen können Filterprogramme eingesetzt werden, mit denen der Zugriff auf bestimmte Arten von Angeboten im Internet erschwert wird. Außerdem können Adressen von Angeboten mit unerwünschtem Inhalt in eine Sperrliste eingetragen werden.

**Ist eine Kontrolle der Internet-Nutzung erlaubt?**

Der Zugang zum Internet vom Schul-PC aus sollte grundsätzlich nur über geeignete und sichere Zugänge und differenzierte Berechtigungskontrollen eröffnet werden. Besondere Datenschutzprobleme ergeben sich aus den vielfältigen Nutzungsspuren, die im eigenen System gespeichert und ausgewertet werden können. Hierzu gehören auch diejenigen Protokolldaten über Zugriffe von Lehrkräften der Schule, die beispielsweise Aufschluss über Zeit, Dauer und Partner des Kontakts einschließlich der ausgewählten Seiten geben und deren Auswertung möglicherweise zur Verhaltenskontrolle geeignet ist. Derartige Verfahren zur automatisierten Verarbeitung von personenbezogenen Daten Beschäftigter unterliegen der Mitbestimmung. Generell gilt hier, dass Speicherungen sachlich und zeitlich auf den für Sicherungs- und Abrechnungszwecke unumgänglich notwendigen Umfang begrenzt werden sollten und dass die Daten sicher zu verwahren und vertraulich zu behandeln sind. Die Aufgabe des Systemverwalters zur Durchsicht der Protokolle und zur Verfolgung von Anhaltspunkten für Straftaten oder Pflichtverletzungen sollte schriftlich festgelegt werden, z. B. in der Nutzungsordnung der Schule. Lehrerinnen und Lehrer können im Unterricht Einsicht in die Netzaktivitäten ihrer Schülerinnen und Schüler nehmen. Es besteht jedoch keine generelle Überwachungspflicht. Lehrkräfte haben selbstverständlich keine generelle Einsichtsberechtigung in die Protokolle aller Netzaktivitäten der Schule.

**Was ist bei privater Nutzung des Internet-PC der Schule zu beachten?**

Wird eine private Nutzung zugelassen, handelt die Schule auch den eigenen Lehrkräften gegenüber als Telediensteanbieter und unterfällt damit den Pflichten nach dem Teledienstgesetz und dem Teledienstedatenschutzgesetz. Die Schule hat besondere Sicherungs- und Kontrollbefugnisse einzurichten, weil anders als im dienstlichen Verkehr eigenständige Rechte der Bediensteten betroffen werden. Alle schulischen Nutzer sind vorab über Art, Umfang, Ort und Zweck der Verarbeitung zu unterrichten. Die private Kommunikation am Internet-PC der Schule unterliegt dem Fernmeldegeheimnis entsprechend § 85 des Telekommunikationsgesetzes (TKG). Danach darf z. B. der private E-Mail-Verkehr grundsätzlich nicht überwacht werden. Es ist - besonders wenn der Zugang über einen zentralen Server erfolgt - sorgfältig darauf zu achten, dass anfallende Verbindungsdaten abgeschottet bleiben und nicht zweckwidrig verwendet werden. Eine Vollprotokollierung und die Kenntnisnahme von privaten Mail-Inhalten sind nicht statthaft. Ist eine technische Trennung von privater und schulischer Nutzung nicht möglich, so ist die gesamte Kommunikation als privat anzusehen und unterfällt damit insgesamt dem Fernmeldegeheimnis.

**Was bedeutet Anbieterkennzeichnung?**

Das Mediendiensterecht verpflichtet Informationsanbieter, die Verantwortlichen zu bezeichnen. Die Anbieterkennzeichnung muss Name und Anschrift, bei Personenvereinigungen auch Name und Anschrift des Vertretungsberechtigten enthalten. Die Kennzeichnung schafft aus Datenschutzsicht Transparenz. Sie sollte dementsprechend gut erkennbar und vollständig in das Internet-Angebot eingestellt werden. Die Anbieterkennzeichnung sollte von jeder Webseite aus erreichbar sein.

**Was ist eine Datenschutzpolicy?**

Das Teledienste- und das Mediendiensterecht verpflichten die Informationsanbieter dazu, die Nutzer vor einer Erhebung personenbezogener Daten über Art, Umfang, Ort und Zweck der Erhebung, Verarbeitung und Nutzung seiner Daten zu unterrichten. Diese Pflicht lässt sich in vielen Fällen umsetzen, wenn auf der Leitseite des Internetangebots Hinweise zum Umgang mit personenbezogenen Daten gegeben werden (Datenschutz-Policy). Dies ist immer dann zu erfüllen, wenn z. B. eine Online-Registrierung verlangt wird, wenn sonstige Formulare online ausgefüllt werden können oder wenn mittels E-Mail mit der Schule kommuniziert werden kann. Auch der Gebrauch von Cookies sollte erläutert werden. *(www.lfd.niedersachsen.de)*

**Was sind Cookies?**

Cookies (= Keks) sind kleine Datensätze, die im Internet häufig zusammen mit den eigentlich angeforderten Daten auf dem Computer des Nutzers abgelegt werden. Dadurch möchte der Anbieter im einfachsten Fall einen wiederholten Zugriff eines Nutzers auf sein Internet-Angebot erkennen, um auf die besonderen Wünsche des Nutzers eingehen zu können. Aus geschickt gewählten Cookies können jedoch auch Nutzungsprofile erstellt werden, die Auskunft über den Nutzer geben und ihn so als geeignete Zielperson für Werbebotschaften erkennbar machen. Eine Manipulation des Computers über die Speicherung und Abfrage der Cookie-Daten hinaus ist zwar direkt nicht möglich; da diese Daten ab er auch benutzerbezogene Passwörter für Web-Seiten umfassen können, sind Angriffe über aktive Elemente (z. B. ActivX-Control) nicht auszuschließen. Vielfach geben Internet-Anbieter keine Hinweise auf ihr Tun; der Datenaustausch erfolgt im Hintergrund, ohne dass der Nutzer z. B. über Inhalt, Zweck, Umfang, Speicherdauer oder Zugriffsmöglichkeit von Cookies informiert wird. Nutzer haben durch richtige Konfiguration der Browser die Möglichkeit auf die Cookie-Speicherung Einfluss zu nehmen. Sie können bestimmen, dass Cookies vor Speicherung angezeigt und genehmigt werden müssen und nicht automatisch akzeptiert werden. Sie können sich die bereits gespeicherten Cookies ansehen (z. B. Datei cookies.txt bei Netscape-Browser) und sie, ohne Nachteile fürchten zu müssen, wieder löschen.

**Was ist eine Firewall?**

Unter einer Firewall („Brandschutzmauer“) verstehen wir eine Schwelle zwischen zwei Netzen, die überwunden werden muss, um Systeme im jeweils anderen Netz zu erreichen. Die Hauptaufgabe besteht darin zu erreichen, dass jeweils nur zugelassene Aktivitäten möglich sind und dass Missbrauchsversuche frühzeitig erkannt werden. Üblicherweise werden dabei die Teilnehmer des internen Netzes (hier: im Schulnetz) als vertrauenswürdiger angenommen als die Teilnehmer des externen Netzes (hier: aus dem

Internet). Die Firewall besteht aus Hard- und Software, seine Stärke hängt wesentlich von der korrekten Administration der Firewall ab. Nähere Einzelheiten zu unterschiedlichen Technologien und Empfehlungen zum datenschutzgerechten Betrieb finden Sie unter www.tec.informatik.uni-rostock.de/RA/LFD-MV/ak_tech/orhilfen/internet/ohint_iv.html

**Was ist eine Insellösung?**

Bei einer Insellösung (stand-allone) wird ein einzelner, nicht lokal vernetzter Rechner per Modem oder ISDN-Anschluss über einen Zugangs-Anbieter (Access-Provider) an das Internet angeschlossen. Diese Variante spielt besonders bei kleinen Behörden, bei Schulen und im privaten Bereich eine große Rolle. Bei eventuellen Angriffen besteht ein Sicherheitsrisiko nur für den einzelnen Rechner. Durch entsprechende technische und organisatorische Maßnahmen lässt sich das Risiko reduzieren (z. B. Festplattenverzeichnisse nicht für den Zugang über das Netz freigeben, den Rechner ausschließlich für den Zugang zum Internet nutzen). Diese restriktive Lösung ist für die Fälle geeignet, in denen die verbleibenden Restrisiken anderer Modelle als zu hoch eingeschätzt werden. Eine vollständige Systemtrennung zwischen Internet und der Verarbeitung personenbezogener Verwaltungsdaten der Schule schützt diese Daten optimal, sie sollte in jedem Falle gewählt werden.

**Wie kann man vertraulich e-mailen?**

Eine E-Mail passiert auf ihrem Weg durch das weltweite Internet viele Stationen, an denen sie abgefangen, mitgelesen oder auch verändert werden kann und von der niemand sicher sein kann, dass sie von derjenigen Person stammt, deren Namen und Adressen vom Mailprogramm angezeigt werden. In private und vertrauliche Nachrichten kann eingesehen werden, Nachrichten können verändert und verfälscht werden und es können Kommunikationsprofile erstellt werden. Jeder Internetnutzer sollte sich durch eigene Schutzmaßnahmen sichern. Gefahren können nur durch Verschlüsselungen und elektronische Signaturen eingeschränkt werden. Meine Empfehlungen zum gesicherten Einsatz von E-Mail sind:

- Innerhalb der Schule sollten klare Regeln in Bezug auf Verwendung von E-Mail definiert werden.
- Bei der Übermittlung von sensiblen bzw. vertraulichen Informationen im Internet über E-Mail sollten auf jeden Fall Verschlüsselungsverfahren eingesetzt werden.
- Bei Teilnahme an Diskussionsforen oder Umfragen per E-Mail sollten Anonymous Remailer eingesetzt werden, wenn durch die Namensnennung die Privatsphäre gefährdet würde.
- Anti-Viren-Programme müssen regelmäßig aktualisiert werden.
- Produkte (MailGuard) zum Durchsuchen von ein- und abgehenden E-Mails nach Viren sollten eingesetzt werden.
- Bei Verwendung älterer Versionen von MS-Office (bis Version 7) sollte der Mime-Type application/msword bzw. x-msword entfernt werden, um ein automatisches Starten der Applikation und somit den Start von vorhandenen Makros zu verhindern.
- Der Austausch von Dokumenten in Formaten, die Makros unterstützen, sollte vermieden werden. Statt dessen können Formate wie RTF oder HTML verwendet werden.
- Falls empfangene Word-Dokumente nur betrachtet werden sollen, kann das Programm "Wordview" verwendet werden, das die Ausführung von Makros nicht unterstützt.
- Um einen Verlust von Daten durch Virenbefall vorzubeugen, muss ein schlüssiges Backup-Konzept entwickelt und umgesetzt werden.

**Wie funktionieren Verschlüsselungen und elektronische Signaturen?**

PGP (Pretty Good Privacy) und PEM (Privacy Enhanced Mail) sind z. B. zwei Verfahren, die das Verschlüsseln bzw. Signieren von Nachrichten ermöglichen. Sie beruhen auf dem "Zwei-Schlüssel-Prinzip", bei dem jeder Nutzer ein Schlüsselpaar besitzt, einen geheimen und einen öffentlichen Schlüssel.

Will Nutzer A an Nutzer B eine verschlüsselte Nachricht schicken, so verschlüsselt A diese Nachricht mit dem öffentlichen Schlüssel von B. Nur B kann die empfangene Nachricht mit seinem geheimen Schlüssel, den nur er kennt, entschlüsseln. Um auch die Authentizität des Absenders A überprüfbar zu machen, ist eine Signierung der Nachricht durch A erforderlich. Hierzu verschlüsselt der Nutzer A eine durch sogenanntes Hashing gebildete Quersumme der Nachricht mit seinem geheimen Schlüssel und schickt diese mit. Empfänger B kann diese Quersumme mit dem öffentlichen Schlüssel von A entschlüsseln. Gleichzeitig kann B durch Hashing eine Quersumme der von ihm bereits entschlüsselten Nachricht bilden und die beiden Quersummen vergleichen. Bei Übereinstimmung ist die Nachricht unverändert und der Absender ist wirklich der Besitzer des öffentlichen Schlüssels.

**Was bedeutet das Recht auf informationelle Selbstbestimmung?**

Das Recht auf informationelle Selbstbestimmung umfasst die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. Ziel des Niedersächsischen Datenschutzgesetzes (NDSG) ist dieser Grundrechtsschutz. Er ist Auslegungsmaßstab für die Bestimmungen des NDSG selbst, aber auch für datenschutzrechtliche Bestimmungen in anderen Rechtsvorschriften. Er führt im Zweifel zu einer für das informationelle Selbstbestimmungsrecht günstigen Auslegung.

**Was sind personenbezogene Daten?**

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, wie z. B. Name, Anschrift, Alter, Geschlecht, Einkommen, Vermögen, Familienstand, Staatsangehörigkeit, Krankheiten, Zeugnisnoten, Berufsbezeichnung. Eine natürliche Person ist dann bestimmbar, wenn es der datenverarbeitenden Stelle möglich ist, mit Zusatzwissen (unter Umständen unter Heranziehung anderer Datenbestände) die Einzelangaben dieser konkreten Person zuzuordnen.

**Was bedeutet der Begriff Datenverarbeitung?**

Unter Datenverarbeitung ist jeder Umgang mit personenbezogenen Daten zu fassen, das heißt im Einzelnen das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten. Es kommt dabei nicht auf das Speicher- oder Verarbeitungsmedium an. Daten in Akten oder anderen papiergebundenen Unterlagen sind ebenso eingebunden, wie solche auf Bild- oder Tonträgern oder sonstigen elektronischen Speichermedien, wenn sich deren Inhalt auf bestimmte oder bestimmbare Personen bezieht.

**Was versteht man unter Selbstdatenschutz?**

Selbstdatenschutz ermöglicht dem Betroffenen die selbstbestimmte Nutzung von technischen und organisatorischen Schutzinstrumenten. Dazu gehören alle Maßnahmen, die darauf abzielen eine vom Nutzer nicht gewollte Verarbeitung seiner personenbezogenen Daten zu verhindern, z. B. Inhaltsschutz durch Verschlüsselung, Anonymität und Pseudonymität, Transparenz und Selbstbestimmung bei jeder Kommunikation (P3P, Opt in, Opt out). Im erweiterten Sinne gehört dazu auch die Möglichkeit, den eigenen Internet-PC auf Sicherheitsmängel zu untersuchen, z. B. durch meinen Browser-Test unter dem Button Selbsttest.

**Was ist anonym, was ist pseudonym?**

Bei einer echten Anonymisierung ist aus den verbleibenden Daten absolut kein Personenbezug herstellbar (z. B. Statistikdaten nach Löschen der identifizierenden Angaben). Als anonymisiert betrachtet der Gesetzgeber aber Datensätze bereits, wenn zwar noch eine theoretische Möglichkeit zur Repersonifizierung besteht, der Aufwand jedoch unverhältnismäßig groß ist (z. B. bei vielen wissenschaftlichen Arbeiten). Je sensibler die Daten sind, umso größer muss der Aufwand sein, sie zu repersonifizieren.

Eng mit dem Anonymisieren verwandt ist das Pseudonym. Beim Pseudonym besteht allerdings im Gegensatz zum Anonymisieren eine sog. Zuordnungsfunktion (z. B. eine Referenztabelle). Entscheidend für ihre datenschutzrechtliche Bewertung ist, welche Stelle über die Zuordnungsfunktion verfügt.

# Schulen ans Netz

## – mit Sicherheit -

Die Datenschutzbeauftragten des Bundes und der Länder beschäftigen sich intensiv mit der Modernisierung der Verwaltung und versuchen Hilfen für datenschutzgerechte Lösungen zu geben ( so z.B. die Broschüre „**Vom Bürgerbüro zum Internet**"). Die Landesbeauftragte für den Datenschutz des Landes Nordrhein-Westfalen hat vor kurzem eine Orientierungshilfe „**Schulen ans Netz**" erarbeitet, die dieses Anliegen erfüllt. Diese Orientierungshilfe wurde mit ihrem Einverständnis auf niedersächsische Rechtsvorschriften umgestellt und den Besonderheiten niedersächsischer Schulen angepasst.

Landesbeauftragter für den Datenschutz Niedersachsen

# 1 Einleitung

„**Ich bin drin**“, sagt nicht nur Boris, sondern sagen auch viele Schulen, die bereits über einen Internetzugang verfügen. Nahezu alle niedersächsischen Schulen sind inzwischen mit Computern ausgestattet.

Mit der Intensivierung des Interneteinsatzes steigt auch die Zahl der Eingaben zum Thema Datenschutz und Datensicherheit in den Schulen; Schulleitungen und Lehrer/innen, Erziehungsberechtigte und Schüler/innen haben gleichermaßen Beratungsbedarf. Fragen zum datenschutzgerechten und sicheren Umgang mit dem Medium Internet werden leider oft erst gestellt, wenn es zu spät ist. Müssen es sich Lehrer/innen gefallen lassen, dass ihre Namen auf der Schulhomepage veröffentlicht werden? Wie konnte es passieren, dass ein Schüler vom häuslichen Computer aus Fotos von Lehrkräften auf der Schulhomepage virtuell verfälscht, und wer ist dafür verantwortlich? Wer hat zu entscheiden, ob die Daten einer 16-jährigen Schwimmschulmeisterin auf der Schulhomepage veröffentlicht werden dürfen? Dürfen Lehrkräfte private E-Mails ihrer Schüler/innen lesen? Was tun, wenn Minderjährige Nazi- oder Pornoseiten auf dem Schulcomputer aufrufen?

Die Chancen des Internets auch und gerade für Schulen sind unbestritten. Alle Beteiligten sollten sich schon vor dem Online-Start der Risiken des Surfens, Chattens und Mailens im Netz bewusst sein und angemessene Sicherheitsmaßnahmen überlegen. Jede Schule sollte verbindliche Regeln festlegen, damit alle Beteiligten wissen, wer das Internet in der Schule wann und wie nutzen darf, welche Kontrollen und welche Sanktionen vorgesehen sind.

Diese Orientierungshilfe kann nicht allen Aspekten des Mediums Internet im Hinblick auf Medien- und Urheberrecht, Jugendschutz, Erziehungs- und Strafrecht Rechnung tragen; sie beschränkt sich vielmehr auf die Gesichtspunkte des Datenschutzes und der Datensicherheit. Da jedoch auch hier die Probleme so vielschichtig und bunt sind wie die Möglichkeiten und Gefahren, die das Internet bietet, können selbstverständlich nicht alle Fallkonstellationen abschließend dargestellt und behandelt werden. Ziel ist es vielmehr, unnötige Crashs auf der Schul-Datenautobahn zu verhindern.

# 2 Internet im Unterricht

## 2.1 Gegenstand des Unterrichts

Das Medium Internet sollte in den Schulen nicht nur Lehrmittel, sondern auch Gegenstand des Unterrichts sein. Dabei ist nicht in erster Linie die Vermittlung technischer Fertigkeiten gemeint, zumal für viele Schüler/innen der technische Umgang mit dem Internet ohnehin längst selbstverständlich ist. Wer heute 10-Jährigen erklären will, wie sie „ins Netz kommen“ und surfen können, was eine Homepage oder ein Chatroom ist, wird in der Regel bestenfalls belächelt werden. Erziehung zu Medienkompetenz und Selbstverantwortung im Umgang mit dem Internet muss vielmehr vor allem auch bedeuten, die Schüler/innen über den Tellerrand der bloßen Technik hinaus mit dem Internet als Medium, seiner Funktionsweise, seinen Risiken und Gefahren vertraut zu machen, die Einsatzmöglichkeiten (auch) kritisch zu hinterfragen und den datensicheren Umgang zu erlernen und zu trainieren. Es geht dabei um die Erkenntnis, dass nicht nur der Missbrauch, sondern auch der Gebrauch von Computern riskant ist.

Erziehung zu Medienkompetenz und Selbstverantwortung im Umgang mit dem Internet unter den Ge-

sichtspunkten des Datenschutzes und der Datensicherheit – ein hehres Ziel, aber was bedeutet das konkret für die Unterrichtspraxis? Schüler/innen sollten – und zwar nicht nur im Informatikunterricht – vor dem Online-Start auf jeden Fall mit folgenden Basisinformationen vertraut gemacht werden.

### 2.1.1 Datenschutz und (Selbst-) Verantwortung

Internet-Angebote öffentlicher Stellen sind rechtlich gesehen entweder Teledienste (geregelt im Teledienstegesetz und im Teledienstedatenschutzgesetz) oder Mediendienste (geregelt im Mediendienste-Staatsvertrag). **Teledienste** sind alle elektronischen Informations- und Kommunikationsdienste, die für eine **individuelle Nutzung** von kombinierbaren Daten, wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt. § 2 Abs. 2 TDG nennt einige Beispiele, wie etwa Telebanking, Datenaustausch, Angebote zur Nutzung von Tele spielen und Angebote von Waren- und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit. **Mediendienste** sind die an die **Allgemeinheit** gerichteten Informations- und Kommunikationsdienste, wie z.B. die Homepage einer Schule mit allgemein abrufbaren Informationen, Messergebnisse in Text und Bild, Fernsehtext und vergleichbare Textdienste. Da die Datenschutzregelungen für Tele- und Mediendienste in TDG/TDDSG und MDStV weitgehend identisch sind, kann die schwierige Unterscheidung zwischen Telediensten und Mediendiensten bei Internetangeboten öffentlicher Stellen in der Regel dahingestellt bleiben.

Daten anderer Personen dürfen ohne gesetzliche Grundlage oder wirksame Einwilligung nicht verarbeiten werden. Eine Schülerin darf deshalb nicht ohne Einwilligung ihres Freundes (bzw. seiner Eltern) sein Bild ins Internet stellen. Ein Schüler darf nicht – auch nicht spaßeshalber – einfach die persönlichen Informationen über seine Lehrer/innen auf der schuleigenen Homepage verändern. Geben Schüler/innen ihren Namen und ihre Anschrift im Internet preis, laufen sie Gefahr, dass andere Internetnutzer/innen diese Daten ungefragt für eigene Zwecke nutzen und sie etwa mit einer wahren Flut von Werbezusendungen überschütten. Richten sie eine eigene Homepage ein, werden sie Telediensteanbietern und müssen einige medien- und datenschutzrechtliche Verpflichtungen erfüllen.

Gegenstand des Unterrichts sollte deshalb die Vermittlung datenschutzrechtlichen Grundlagenwissens sein:

- Was bedeutet Recht auf informationelle Selbstbestimmung? Das Recht, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.
- Was sind personenbezogene Daten? Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.
- Was bedeutet Datenverarbeitung? Das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten.
- Unter welchen Voraussetzungen ist eine Einwilligung wirksam, wer ist einwilligungsfähig? (siehe hierzu unter 4.1.1).

Weitere Anhaltspunkte zu datenschutzrechtlich relevanten Fragen, die (auch) die Schüler/innen und ihre Nutzung des Internets betreffen, können den anderen Kapiteln dieser Orientierungshilfe entnommen werden; im Übrigen wird auf das Informationsmaterial verwiesen, das sich unter www.lfd.niedersachsen.de befindet.

### 2.1.2 Risiken der Internetnutzung

Die Schüler/innen müssen sich, bevor sie im Internet surfen, spielen und Nachrichten austauschen, bewusst machen, dass sie dabei Spuren hinterlassen und grundsätzlich weltweit die Möglichkeit besteht, auf alle von ihnen preisgegebenen personenbezogenen Daten Zugriff zu nehmen. Eine vollständig anonyme Nutzung ist dem Internet bereits aus abrechungstechnischen Gründen bis heute grundsätzlich fremd. In aller Regel wird es personenbezogen, personenbeziehbar über einen Usernamen/User-ID oder unter Gruppenkennungen genutzt. Daher hinterlässt etwa jedes Aufblättern von Homepages Datenspuren. Bei Kommunikationsvorgängen – etwa per E-Mail – werden Daten in der Regel nicht gesichert, so dass sie auf ihrem Weg durch das öffentliche Netz ausgespäht werden können.

Aus der unsicheren Infrastruktur des Internet erwachsen Gefahren für die Vertraulichkeit und inhaltliche Integrität der übertragenen Daten. Zudem können bestehende Schwachstellen der Endgeräte ausgenutzt werden, um sich mit relativ wenig Aufwand unbemerkt einen unberechtigten Zugang zu dem kommunizierenden Rechner zu verschaffen. So können Daten ausgespäht, aber auch manipuliert oder gelöscht werden. Unverschlüsselte und nicht digital signierte Nachrichten sind so leicht les-, verändern- und unterdrückbar wie eine maschinengeschriebene Postkarte, die außerdem auch eine andere Person geschrieben haben kann. Gewissheit über die Richtigkeit von Inhalt und Herkunft gibt es also nicht.

Beispiele für die "gläserne" Internet-Nutzung:

- Mit Suchprogrammen wie etwa "deja news" lassen sich Profile aller in Newsgroups Kommunizierenden erstellen. Auf diese Weise können zum Beispiel Hobbys und persönliche Neigungen erfasst werden.

- Im Internet werden Datensätze, sogenannte "cookies", oft ohne Wissen der Nutzenden auf der Festplatte des eigenen Rechners hinterlassen und bei der nächsten Einwahl möglicherweise automatisch wieder aufgerufen; über diesen Mechanismus kann ein Profil der Nutzer/innen erstellt werden, ohne dass diese es merken.

- Wer sich im Internet – selbst unter so harmlosen Rubriken wie etwa dem "Treffpunkt" oder ähnlichem – mit Namen, Adresse oder anderen Erreichbarkeitsdaten aufnehmen lässt, sollte damit rechnen, dass dies auch unerwünschte Nutzungen (etwa Übersendung von Werbung) zur Folge haben kann. Dies gilt auch für die schuleigene Homepage.

Am Beispiel der (unsicheren) E-Mail, die auf ihrem Weg durch das weltweite Internet viele Stationen passiert, an denen sie abgefangen, mitgelesen oder auch verändert werden kann und von der niemand sicher sein kann, dass sie von derjenigen Person stammt, deren Namen und E-Mail-Adresse vom Mailprogramm angezeigt wird, lassen sich Risiken und Gefahren gut verdeutlichen.

### 2.1.3 Schutzmaßnahmen

Es ist wichtig, die Schüler/innen altersgerecht über Schutzmaßnahmen zu unterrichten und diese mit ihnen einzuüben. Schon die jüngsten Internetnutzer/innen müssen wissen, dass sie ihre personenbezogenen Daten nicht im Internet preisgeben sollten, wenn sie zum Beispiel Kinderclub-Seiten aufsuchen und hier im Rahmen eines Spiels nach ihrem Vor- und Nachnamen, ihrer Postanschrift und ihrem Ge-

burtsdatum gefragt werden. Denn mit solchen Informationen werden unter Umständen zielgruppengerecht Werbungsmaterialien ausgesucht und übersandt.

Mit älteren Schüler/innen sollten Maßnahmen zum Schutz von Vertraulichkeit (Verschlüsselungsverfahren), Integrität und Authentizität (Signierverfahren) besprochen und trainiert werden. Diese und weitere Schutzmaßnahmen (gegen Löschen oder Verlust von E-Mails, gegen Viren und Trojanische Pferde) lassen sich wiederum anschaulich am Beispiel der E-Mails darstellen. Bei der Teilnahme an Foren und Chats aller Art, aber auch zum Surfen im Internet ist die Verwendung eines Pseudonyms nützlich. Weitere Informationen sind unter **www.datenschutzzentrum.de/anon/** und **http://anon.inf.tu-dresden.de** sowie unter **www.bsi.de** zu finden.

**Allgemeine Empfehlung:** Schüler/innen sowie Lehrer/innen sollten ihre personenbezogenen Daten im Internet grundsätzlich nicht preisgeben. Es wird empfohlen, bei individueller Nutzung nach draußen – etwa in Chatrooms – Pseudonyme zu verwenden, auch wenn bei einem Internet-Zugang über einen Schul-PC meist nur die Kennung des Schul-PC in Erscheinung tritt. Ebenso sollten Nachrichten verschlüsselt werden, wenn ihr Inhalt niemanden etwas angeht.

## 2.2 Nutzung im Unterricht

Die Möglichkeiten der Internetnutzung im Unterricht sind bunt und vielfältig. Schüler/innen können im Sozialkundeunterricht Informationsmaterial zum Thema „Rechtsextremismus“ zusammenstellen und im Chat-Forum „Fixerstuben – Pro und Contra“ mitdiskutieren, PC-gestützt Englisch-Vokabeln lernen und eigenständig die neue Rechtschreibung trainieren, am Monitor physikalische Experimente simulieren sowie den Aufbau der DNA nachvollziehen, mit ihrer ausländischen Partnerschule Kontakt via E-Mail pflegen und im Kunstunterricht virtuell durch die Uffizien spazieren.

Grundsätzlich ist die Nutzung aller schulintern erlaubten Internetdienste im Rahmen des Unterricht zulässig; maßgeblich sind im konkreten Fall allerdings die Anweisungen der unterrichtenden Lehrkraft, die für die Schüler/innen verbindlich sind. Die Lehrer/innen haben die Einhaltungen ihrer Anweisungen zu kontrollieren.

Im Unterricht können Lehrer/innen Einsicht in die Netzaktivitäten der Schüler/innen nehmen. Die E-Mail-Kommunikation im Rahmen des Unterrichts liegt in aller Regel in der Verantwortung der Lehrkraft. Allerdings reicht ihre Verantwortung nur so weit wie ihre Aufsichtspflicht geht und sie Kenntnis von dem E-Mail-Verkehr haben kann. Es besteht weder eine flächendeckende Überwachungspflicht noch ein generelles Überwachungsrecht. Jede Kontrolle der Kommunikation muss für die Schüler/innen transparent sein.

Der Lehrkraft obliegt es, die Einhaltung des Datenschutzes im Rahmen des Unterrichts sicherzustellen. Wird im Fremdsprachenunterricht mit der ausländischen Partnerschule kommuniziert, darf grundsätzlich die Übermittlung personenbezogener Daten zugelassen werden, soweit diese für die unterrichtsbezogene Kommunikation notwendig sind. Nur mit wirksamer Einwilligung der Betroffenen können weitere Daten mitgeteilt werden, wenn beispielsweise Angaben zu Austauschschüler/innen an die Partnerschulen übermittelt werden sollen.

Die E-Mail-Adresse ist so zu gestalten, dass sie eine Zuordnung der Nachricht zur Schule und zur Klasse erkennen lässt und damit deutlich macht, dass die Mails nicht ausschließlich privater Natur

sind. Die Schüler/innen können E-Mails unter einer Sammelkennung (zum Beispiel Klasse8a@Beispielschule.de) versenden; sie dürfen diese Nachrichten auch verschlüsselt übermitteln, soweit die Lehrkraft von den Mitteilungen zuvor Kenntnis genommen hat. Offene E-Mails können nach Entscheidung der Absendenden namentlich oder pseudonym geschickt werden. Die Empfänger/innen müssen erkennen können, dass die Nachricht einem größeren Kreis und nicht nur einer bestimmten Person zuzuordnen ist, damit sie sich bei der Antwort darauf einstellen können, dass auch diese von einem größeren Kreis gelesen werden kann. Der Empfang der E-Mails an die im Unterricht benutzte Box geschieht immer offen, so dass die Nachrichten auch von der Lehrkraft gelesen werden können. Eine Kenntnisnahme sollte jedoch vorher angekündigt werden.

Neben einer Kontrolle durch die verantwortliche Lehrkraft kann im Übrigen eine weitere Kontrolle – auch der Lehrkraft selbst – stattfinden. So protokolliert das System automatisch die während der Nutzung durchgeführten Tätigkeiten im System. Eine uneingeschränkte Nutzung dieser Protokolldaten zu Kontrollzwecken wäre unverhältnismäßig und somit unzulässig. Eine gezielte Kontrolle sollte nur erfolgen, wenn dafür ein Anlass gegeben ist. Eine allgemeine, ungezielte Kontrolle durch den Systemverwalter könnte z.B. stichprobenartig, nicht auf einzelne Nutzer/innen bezogen die häufig angesurften Internet-Angebote ermitteln. Eine Auswertung der Protokolldateien könnte auch daraufhin vorgenommen werden, welche Seiten ohne Bezug auf Unterricht oder Schule besonders häufig besucht werden. Ergeben sich dabei Auffälligkeiten in signifikantem Umfang, sollten die Beteiligten zunächst pauschal auf die Unzulässigkeit dieses Verhaltens hingewiesen werden. Gleichzeitig sollte angekündigt werden, dass bei Fortdauer der Verstöße eine personalisierte Kontrolle stattfinden wird. Fördert eine spätere Stichprobe tatsächlich weitere Zuwiderhandlungen gegen die Nutzungsordnung zutage, kann festgestellt werden, von welchem Rechner aus zu welcher Zeit solche Zugriffe stattgefunden haben.

In jedem Fall muss für die Betroffenen bereits im vorhinein transparent sein, welche Kontrollmaßnahmen vorgesehen sind. Hierzu sollte eine konkrete Festlegung in der Nutzungsordnung erfolgen (Welche Protokolldaten werden wo und wie lange gespeichert, wer darf sie wann nutzen).

## 3 Internetnutzung außerhalb des Unterrichts in der Schule

Immer mehr Lehrer/innen und Schüler/innen möchten in der Schule auch nach Unterrichtsschluss und in den Freistunden unbeschränkt im Internet surfen, chatten und mailen dürfen. Die einen brauchen noch Material zur Unterrichtsvorbereitung, wollen einen Blick auf die Börsen der Welt werfen oder nachschauen, wann ihr Bus nach Hause fährt, die anderen ein Referat vorbereiten, die neuesten Bundesliga-Ergebnisse abfragen oder „Moorhühner jagen“. Die Schülerzeitungsredaktion tagt selbstverständlich außerhalb des Unterrichts und möchte die neueste Ausgabe auch im Internet veröffentlichen. Private E-Mails, von denen niemand in der Schule Kenntnis nehmen soll, werden in der großen Pause noch schnell verschickt bevor die nächste Stunde beginnt.

### 3.1 Grundsatzentscheidung und Verantwortlichkeit

Die Entscheidung darüber, ob und in welchem Umfang den Lehrer/innen und Schüler/innen die Nutzung des Internetanschlusses auch zu privaten Zwecken außerhalb des Unterrichts gestattet sein soll, obliegt der Schule bzw. der Schulkonferenz. Die Entscheidung sollte jedoch vorab grundlegend diskutiert, sorgfältig abgewogen und in der Nutzungsordnung der Schule festgeschrieben werden, da sie weitreichende rechtliche Folgen und damit eine Reihe von Pflichten für die Schule auslöst.

Wenn eine Schule Internetdienste auch für private Zwecke zulassen will, unterfällt die private Telekommunikation am Lehrerplatz bzw. am Internet-PC der Schule dem Fernmeldegeheimnis. Das Fernmeldegeheimnis ist durch Art. 10 Grundgesetz (GG) und § 85 Abs. 1 Telekommunikationsgesetz (TKG) geschützt. Relevant wird dies z.B. für die Frage, ob die Schule Lehrer/innen sowie Schüler/innen den privaten E-Mail-Verkehr gestatten möchte. Das Fernmeldegeheimnis umfasst den Kommunikationsinhalt und die näheren Umstände der Telekommunikation, insbesondere die Tatsache, ob und wann zwischen welchen Personen und Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist. Wenn die private Internetnutzung in der Schule erlaubt ist, darf damit grundsätzlich niemand den privaten E-Mail-Verkehr der Lehrer/innen bzw. der Schüler/innen überwachen. Dagegen unterliegen dienstliche E-Mails der Schulleitung nicht dem Fernmeldegeheimnis.

Die Schule darf allerdings aus Sicherheitsgründen alle ein- und ausgehenden E-Mails auf Virenbefall automatisiert kontrollieren, allerdings ohne den Inhalt selbst zu sichten. Vorgesetzte dürfen nicht auf die an die Lehrer/innen gerichteten privaten E-Mails inhaltlich zugreifen und diese lesen. Sie dürfen nicht kontrollieren, wer eine private Nachricht an wen versendet oder von wem bekommen hat. Da dies jedoch einer eingehenden E-Mail nicht ohne weiteres angesehen werden kann, ist bei zugelassener privater Nutzung die gesamte Telekommunikation als private Nutzung anzusehen. Auch die freie E-Mail-Kommunikation der Schüler/innen außerhalb des Unterrichts in der Schule unterliegt dem Fernmeldegeheimnis und ist deshalb einer Kontrolle entzogen. Eine Kontrollbefugnis der Schule lässt sich nicht aus der Aufsichtspflicht nach Erziehungsauftrag herleiten, da diese Pflicht nur so weit reicht, wie Lehrkräfte Kenntnis von E-Mail-Nachrichten nehmen dürfen. Wegen des Fernmeldegeheimnisses sind sie dazu bei privaten Mails nicht befugt. Hat die Schule den Verdacht, dass private E-Mails mit strafrechtlich relevantem Inhalt versandt werden oder erlangt sie gar positive Kenntnis von einer strafrechtlich relevanten Kommunikation, bleibt – neben der schulinternen Maßnahme eines (vorläufigen) Ausschlusses von der Nutzung – nur der Weg, Strafanzeige zu erstatten.

Wenn die Schule den privaten Gebrauch des Internets außerhalb des Unterrichts erlaubt, ist sie insoweit Diensteanbieterin im Sinne des Tele- und Medienrechts (§ 3 Nr. 1 TDG und des § 2 Nr. 1 TDDSG bzw. des § 3 Nr. 1 MDStV). Deshalb hat sie medienrechtliche Pflichten zu erfüllen. Dazu gehören insbesondere die Wahrung der Unterrichtungspflichten (§§ 3 Abs. 5 TDDSG, 12 Abs. 6 MDStV) und weitere Anbieter-Pflichten (§§ 4 TDDSG, 13 MDStV). So muss sie allen berechtigten Nutzer/innen auf deren Wunsch Auskunft über die zu ihrer Person gespeicherten Daten erteilen (§ 7 TDDSG, 16 MDStV).

Fraglich ist, ob und inwieweit die Schule darüber hinaus für das Nutzungsverhalten ihrer Schüler/innen im Internet verantwortlich ist. Die medienrechtliche Verantwortung als Diensteanbieterin ist grundsätzlich in §§ 5 TDG, 5 MDStV geregelt. Für eigene Inhalte ist sie voll verantwortlich. Wenn sie fremde Inhalte zur Nutzung bereithält, trifft sie eine (Mit-) Verantwortung, wenn ihr diese Inhalte bekannt sind und es ihr technisch möglich und zumutbar ist, deren Nutzung zu verhindern. Für fremde Inhalte, zu denen sie lediglich den Zugang vermittelt, ist sie nicht verantwortlich.

Auch wenn sie nicht für die fremden Inhalte verantwortlich ist, wird jede Schule bestrebt sein zu verhindern, dass ihre Schüler/innen beispielsweise sexistische, gewaltverherrlichende oder diskriminierende Web-Seiten aufrufen. Bloße Verbote und Hinweise auf die schul- oder gar strafrechtliche Relevanz des verbotswidrigen Verhaltens dürften allein nicht ausreichen. Einen gewissen – wenn auch nicht umfassenden – Schutz vermögen Filterprogramme zu schaffen, mit denen der Zugriff auf bestimmte Arten von Angeboten im Internet über den Schulserver zumindest erschwert wird. Außerdem können Adressen von Angeboten mit unerwünschtem Inhalt in eine Sperrliste eingetragen werden, wodurch der direkte Zugriff unterbunden wird.

Einzelheiten sind den gesetzlichen Regelungen im TKG, TDG, TDDSG und dem MDStV und meiner Orientierungshilfe „Tele- und Mediendienste“ unter www.lfd.niedersachsen.de zu entnehmen. Eine

vertiefende Darstellung findet sich bei Johann Bizer „Schüler am Netz: Rechtsfragen beim Einsatz von Email, Newsgroups und WWW in Schulen“, in: Lernort Multimedia, Jahrbuch Telekommunikation und Gesellschaft Band 6 1998, S. 244 ff.

### 3.2 Zugangskontrollen

Einige Schulen legen in Computerräumen und Medienecken Listen aus, in die sich die Benutzer/innen der PCs mit Namen und weitere Angaben eintragen sollen. Mit solchen Listen werden Daten erhoben und zugleich – wegen der offenen Auslegung – an alle Personen, die Zugang zu diesen Räumlichkeiten haben, bekannt gegeben. Eine solche Datenverarbeitung ist aber nur zulässig, wenn sie zur Aufgabenerfüllung der Schule geeignet und erforderlich ist. Unabhängig davon, dass die Schule grundsätzlich befugt ist, sich vor missbräuchlicher Nutzung ihrer PCs zu schützen, müssen alle organisatorischen Kontrollmaßnahmen ebenfalls den datenschutzrechtlichen Anforderungen genügen. Zweifelhaft ist aber bereits, ob die Eintragung in offen ausliegende Benutzungslisten überhaupt geeignet ist, um Beschädigungen am PC zu verhindern, weil die eingetragenen Benutzer/innen nicht notwendigerweise auch die Beschädigung hervorgerufen haben müssen. Ohne eine zusätzliche (Stichproben-) Kontrolle durch Lehrkräfte oder andere Personen scheint das Problem der Verhinderung von Beschädigungen auch nicht wirklich lösbar zu sein. Ausgelegte Benutzungslisten sollten daher aus dem Verkehr gezogen und eine datenschutzgerechtere Maßnahme getroffen werden.

Empfehlenswert ist die Einrichtung einer Zugangskontrolle, mit der automatisch die PC-Nutzung protokolliert werden kann (z.B. durch Betriebssystem oder mit zusätzlicher Sicherheitssoftware). Der Zugang zum System ist so nur über einen Benutzernamen und die Eingabe eines individuellen Passwortes möglich. Das Passwort sollte so gestaltet sein, dass es nicht ohne weiteres ausgeforscht und von anderen verwandt werden kann. Die Auswertung der Protokolle sollte durch die Systemverwaltung erfolgen, Protokollinhalt und -auswertung sollten in einer Nutzungsordnung festgelegt werden. Die bei der Protokollierung entstandenen Verbindungsdaten dürfen im Übrigen nicht zu Kontrollen der Netzaktivitäten der Nutzer/innen genutzt werden; sie sind frühestmöglich zu löschen. Konkrete Orientierungshilfen und Checklisten zu allen technischen Fragestellungen sind unter www.lfd.niedersachsen.de zu finden.

## 4 Die schuleigene Homepage

Immer mehr Schulen präsentieren sich mit einer eigenen Homepage im Netz. Zu wenig bekannt sind allerdings oft die datenschutzrechtlichen Anforderungen, die sich aus den sogenannten Multimediaregelungen, aber auch aus sonstigen bereichsspezifischen Vorschriften und dem allgemeinen Datenschutzrecht ergeben. Anfragen hatten häufig folgende Probleme zum Gegenstand:

- Welche personenbezogenen bzw. -beziehbaren Daten dürfen unter welchen Voraussetzungen in die Homepage aufgenommen und damit ins Netz eingestellt werden?
- Welche Informationspflichten obliegen der Schule als Anbieterin?

Verantwortlich für die schuleigene Homepage und damit auch für die Einhaltung der datenschutzrechtlichen Bestimmungen ist grundsätzlich die Schulleitung oder die von ihr autorisierte Lehrkraft.

### 4.1 Inhaltsdaten: Was darf ins Internet?

#### 4.1.1 Grundsätzliches

Soweit die Bereitstellung von Daten im Internet ohne Einschränkungen erfolgt, also keine geschlos-

sene Benutzergruppe durch zum Beispiel einen mit Passwort geschützten Zugang gebildet wird, bewirkt dies immer auch eine weltweite Veröffentlichung von Informationen, die von jeder Person mit Internetanschluss aufgerufen und grundsätzlich auch auf den eigenen Rechner heruntergeladen, verändert und genutzt werden können. Deshalb ist besonders sorgfältig zu prüfen, ob die Veröffentlichung personenbezogener Daten auf einer Schul-Homepage datenschutzrechtlich zulässig ist.

Diese Zulässigkeit bestimmt sich nach den datenschutzrechtlichen Bestimmungen des Schulrechts und des Niedersächsischen Datenschutzgesetzes (NDSG). Nach § 4 Abs. 1 NDSG ist die Verarbeitung personenbezogener Daten nur zulässig, wenn

a) eine Rechtsvorschrift sie vorsieht oder

b) die betroffene Person eingewilligt hat.

Die Einwilligung ist die widerrufliche, freiwillige und eindeutige Willenserklärung der betroffenen Person, einer bestimmten Datenverarbeitung zuzustimmen. Sie bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild hervorzuheben. Die Betroffenen sind in geeigneter Weise über den Verwendungszweck der Daten, bei einer beabsichtigten Übermittlung über die Empfänger/innen der Daten aufzuklären; sie sind unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass sie die Einwilligung verweigern und mit Wirkung für die Zukunft widerrufen können.

Unabhängig hiervon ist auch der Grundsatz der Datenvermeidung zu beachten: Die Planung, Gestaltung und Auswahl informationstechnischer Produkte und Verfahren haben sich an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben und weiterzuverarbeiten. Das heißt: Auch wenn die Verarbeitung von personenbezogenen Daten im Internet zulässig ist, sind alternative anonyme oder pseudonyme Verfahren zu wählen, wenn der Zweck der Verarbeitung so in gleicher Weise erreicht werden kann.

### 4.1.2 Daten von Lehrer/innen

Mit ihrer Homepage wollen sich die Schulen – auch und gerade im Wettbewerb mit anderen Schulen – in aller Regel umfassend präsentieren. Dazu gehört für sie oftmals, einen Überblick über Lehrangebote, Fächerspektrum und außerschulische Aktivitäten zu geben, die Zusammensetzung des Kollegiums darzustellen, über direkte Kontaktaufnahmemöglichkeiten zu informieren und zugleich die richtigen Ansprechpartner/innen für bestimmte Tätigkeitsfelder zu benennen.

Anlass zu berechtigtem Ärger gibt es allerdings dann, wenn das komplette Verzeichnis aller Lehrer/innen mit deren Namen und gegebenenfalls weiteren Angaben zur Person ohne weiteres ins Netz eingestellt wird. Wie oben ausgeführt ist eine Veröffentlichung personenbezogener Daten nämlich nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder die betroffene Person eingewilligt hat.

Als Rechtsvorschrift kommt § 101 Abs. 5 Satz 1 Niedersächsisches Beamtengesetz (NBG) in Betracht. Danach darf eine Veröffentlichung personenbezogener Daten von Lehrer/innen im Internet erfolgen, wenn der Dienstverkehr sie erfordert Dies ist bei Lehrkräften zu bejahen. Sie nehmen an der Außenkommunikation der Schule teil und müssen z.B. von Eltern, Schüler/innen und Elternvertretern angesprochen werden können. Allerdings ist die Schule gehalten, die Lehrer/innen vor Einstellung ihrer Daten (Name, Funktion, Unterrichtsfächer, Dienstadresse) über die geplante Veröffentlichung zu

unterrichten. Lehrkräfte können aus besonderen schutzwürdigen persönlichen Gründen der Veröffentlichung gegenüber der Schule widersprechen. In diesem Falle muss die Schule die geltend gemachten Interessen der betroffenen Lehrkraft gegen das schulische Interesse an der Veröffentlichung abwägen. Überwiegen die persönlichen Gründe der Lehrkraft, hat eine Einstellung der Daten ins Internet zu unterbleiben.

Die Veröffentlichung privater Kontaktadressen (private Anschrift, Tel.Nr., E-Mail-Adresse) auf der Homepage der Schule ist selbstverständlich nur mit Einwilligung der Lehrkraft zulässig. Auch die Veröffentlichung von Fotos einer Lehrkraft ist nur mit ihrer Einwilligung zulässig; diese ist schon wegen des Rechts am eigenen Bild erforderlich.

### 4.1.3 Daten von Schüler/innen und Erziehungsberechtigten

Personenbezogene Daten von Schüler/innen (zum Beispiel Klassensprecher/innen, Gewinner/innen eines Wettbewerbs) und von Erziehungsberechtigten (zum Beispiel Vertreter/innen eines Schulmitwirkungsorgans) dürfen grundsätzlich nur mit Einwilligung auf der Homepage veröffentlicht werden. Ob die Daten eines Jugendlichen ins Internet eingestellt werden dürfen, entscheidet allerdings mit seiner wachsenden Reife immer seltener die erziehungsberechtigte Person. Minderjährige Schüler/innen sind in Bezug auf die Erhebung und Verarbeitung ihrer Daten selbst einwilligungsfähig, wenn sie die Bedeutung und Tragweite der Einwilligung und ihrer rechtlichen Folgen erfassen können und ihren Willen hiernach zu bestimmen vermögen. Das wird jedenfalls bei Schüler/innen der Oberstufe regelmäßig der Fall sein.

Für die Einstellung von Fotos auf der Homepage bedarf es – wie bei den Aufnahmen von Lehrkräften – einer zusätzlichen hierauf bezogenen Einwilligung. Wenn also beispielsweise ein Klassenfoto auf einer Homepage veröffentlicht werden soll, müssen zuvor alle abgebildeten Schüler/innen oder – wenn sie selbst noch nicht über die erforderliche Einwilligungsfähigkeit verfügen – deren Erziehungsberechtigte wirksam einwilligen; ist die Vertrauenslehrerin, der Klassenlehrer oder eine andere Person mitfotografiert worden, muss deren Einwilligung ebenfalls eingeholt werden. Fehlt es an einer der erforderlichen Einwilligungen oder ist eine dieser Erklärungen unwirksam, ist die Einstellung des Bildes ins Internet datenschutzrechtlich unzulässig.

Das Einwilligungserfordernis gilt schließlich auch für Web-Angebote an ehemalige Schüler/innen, sich für künftige Einladungen zu Klassen- oder Schultreffen mit ihren Namen, Anschriften, E-Mail-Adressen und dem Abiturjahrgang in die schuleigene Homepage einzutragen oder eintragen zu lassen.

### 4.1.4 Gästebuch, schwarzes Brett und Kontaktlisten

Homepages erfüllen nicht nur einen Informationszweck, sondern bieten sich auch für eine direkte Kommunikation an. So gibt es etwa "Gästebücher", in die Besucher/innen einer Seite sich selbst und ihre Meinung zu bestimmten Fragen eintragen können. Oder Personen, die an spezifischen Fragestellungen interessiert sind, soll über das Netz Gelegenheit gegeben werden, mit anderen Interessierten Kontakt aufzunehmen, wofür entsprechende Listen veröffentlicht werden sollen.

Gästebücher auf der Homepage oder andere elektronische Meinungsäußerungsforen erfüllen dieselbe Funktion wie etwa ein "schwarzes Brett", das in der Schule im Eingangsbereich aushängt. Wer möchte, kann unter vollem Namen, aber auch anonym oder pseudonym Kommentare abgeben – zu welchem Thema auch immer. Ob jedoch solche Kommentare tatsächlich von der bezeichneten Person stammen und ob auch der dokumentierte Inhalt so von ihr gewollt ist, lässt sich sowohl bei realen als auch bei

virtuellen schwarzen Brettern zurzeit nur mit einem Aufwand überprüfen und sicherstellen, der die Idee der spontanen Meinungsäußerung – erst recht, wenn sie auch anonym möglich sein soll – in ihr Gegenteil verkehrt. Den Schulen kann daher nur empfohlen werden, den Nutzer/innen diese Umstände mit einer ausführlichen Information ins Bewusstsein zu rufen. Eine Art Warnhinweis sollte deutlich machen, dass keine Gewähr für die Richtigkeit der zu findenden Angaben übernommen werden kann. Weiter sollte darüber informiert werden, dass die Schule strafrechtlich relevante Meinungsäußerungsinhalte nicht zulässt. Da sie dies in eigener Verantwortung sicherzustellen hat, muss sie neue Einträge unverzüglich unter strafrechtlichen Aspekten prüfen. In der Nutzungsordnung der Schule wäre etwa zu bestimmen, dass der Beitrag gelöscht, die/der Teilnehmende – sofern ermittelbar – ausgeschlossen oder etwa das Gästebuch insgesamt geschlossen werden kann.

Davon zu unterscheiden sind die Fälle, in denen es darum geht, Kommunikationswilligen durch das Bereithalten von Institutionen- und Personenlisten zu bestimmten inhaltlichen Fragestellungen eine direkte Kontaktaufnahme untereinander zu ermöglichen. Das Anliegen ist sicherlich hilfreich, ausgeschlossen sein muss jedoch, dass Personen ungewollt oder sogar ohne ihr Wissen von Dritten in solche Listen eingetragen werden. Ohne die wirksame Einwilligung der/des Betroffenen bzw. einer erziehungsberechtigten Person (vgl. 4.1.1.) ist die Aufnahme personenbezogener Daten in eine solche elektronische Liste unzulässig.

### 4.1.5 Beiträge von Schüler/innen

Da die Schulleitung oder die von ihr beauftragte Lehrkraft für die Homepage verantwortlich ist, ist es insoweit gerechtfertigt, die Veröffentlichung von Beiträgen der Schüler/innen grundsätzlich von einer vorherigen Genehmigung der/des Verantwortlichen abhängig zu machen. Eine solche Genehmigungspflicht kann in der Nutzungsordnung festgeschrieben werden. Ausnahmen gelten für die bereits unter 4.1.4. genannten Rubriken, in die die Schüler/innen selbst und ohne gesonderte Genehmigung Eintragungen vornehmen dürfen. Die Schüler/innen können dabei frei wählen, ob sie mit ihren Namen oder mit Pseudonymen auftreten wollen.

Eine weitere Ausnahme stellt insbesondere die Veröffentlichung der Schülerzeitung auf der Homepage dar. Nicht die Schule, sondern die Redaktion der Schülerzeitung trägt die Verantwortung für deren Inhalt. Um diese Verantwortlichkeit der Zeitungsredaktion deutlich zu machen, wäre beispielsweise eine Veröffentlichung der Schülerzeitung auf einer eigenen Homepage mit eigenem Domainnamen auf dem Schulserver denkbar.

### 4.1.6 Webcams

Es wird immer häufiger üblich, Kameras in öffentlichen und privaten Bereichen aufzustellen und deren Bilder im Internet abrufbar zu speichern. Öffentliche Stellen dürfen dies allenfalls dann tun, wenn die Kameras so aufgestellt sind, dass die anfallenden Bilder keine Daten mit Personenbezug enthalten. Ein Personenbezug ist auf jeden Fall herstellbar, wenn Gesichter, Autokennzeichen oder andere identifizierende Merkmale erkennbar sind oder durch Aufnahmesteuerung oder Bildbearbeitung seitens des Empfängers erkennbar gemacht werden können. In Frage kommen daher allenfalls Übersichtsaufnahmen, die die Herstellung eines Personenbezuges definitiv ausschließen. Dabei spielen Rahmenbedingungen wie Bildausschnitt, Bildschärfe oder Bildfrequenz eine wichtige Rolle. Vorab sollte auf jeden Fall sorgfältig geprüft werden, ob die Informationen, die mittels Webcam gegeben werden sollen, nicht auf andere, **datensparsamere** Weise übermittelt werden können (z.B. durch Fotos, auf denen leere Räume abgebildet sind).

Eine Darstellung personenbeziehbarer Bilder im Internet ist nur dann zulässig, wenn zuvor alle betroffenen Personen bzw. ihre Erziehungsberechtigten wirksam in die Veröffentlichung eingewilligt haben. Da die Bilder von Webcams weltweit abrufbar, speicherbar, aber vor allem auch veränderbar sind und damit ein erhöhtes Gefahrenpotential begründen, sollte der Einsatz von Webcams im Schulbereich grundsätzlich unterbleiben.

## 4.2 Informationspflichten als Anbieterin

Transparenz ist eine wichtige Voraussetzung für den Schutz des Rechts auf informationelle Selbstbestimmung. Nur wenn die Nutzer/innen auch im World Wide Web wissen, wann von wem welche personenbezogenen Daten erhoben, gespeichert, verarbeitet und genutzt werden, können sie ihr Recht auf Selbstbestimmung wahrnehmen. Wer die Homepage einer Schule aufsucht, um sich zu informieren oder mit der Schule zu kommunizieren, muss dementsprechend informiert werden.

Neben der Frage, welche Inhalte in eine Homepage eingestellt werden dürfen, sind auch datenschutzrechtliche Vorgaben für das Angebot von Informations- und Kommunikationsdiensten zu beachten. Solche Vorgaben enthalten das Teledienste- und das Teledienstedatenschutzgesetz (TDG; TDDSG) oder der Mediendienste-Staatsvertrag (MDStV), je nachdem, ob der jeweilige Informations- und Kommunikationsdienst als Teledienst für eine individuelle Nutzung von kombinierbaren Daten bestimmt ist oder ob er als Mediendienst an die Allgemeinheit gerichtet ist und redaktionell gestaltete Beiträge enthält.

### 4.2.1 Anbieterkennzeichnung

Die bunte Web-Welt ist bei genauem Hinsehen verwirrend. Die Anbieterkennzeichnung soll den Nutzer/innen ein Mindestmaß an Transparenz und Information ermöglichen. Nur mit ausreichender Anbieterkennzeichnung ist es möglich, den eigenen datenschutzrechtlichen Auskunftsanspruch nach § 7 TDDSG oder § 16 MDStV geltend zu machen. Auch die Datenschutzbeauftragten sind für eine effektive Kontrolle auf die umfassende und korrekte Kennzeichnung angewiesen.

**Verbindlicher Mindestinhalt der Anbieterkennzeichnung:**

- Name der Anbieterin (der Schule)
- Name der vertretungsberechtigten Person, Name der verantwortlichen Person
- Anschrift (Straße, Hausnummer, PLZ, Ort)
- Bei journalistisch gestalteten Texten:
- Verantwortliche Person (Vor-und Nachname)
- Anschrift (Straße, Hausnummer, PLZ, Ort)
- Verantwortungsbereich

Nach § 6 TDG, § 6 Abs. 1 MDStV haben Diensteanbieter/innen Namen und Anschrift sowie bei Personenvereinigungen und -gruppen auch Namen und Anschrift der vertretungsberechtigten Person anzugeben. Zusätzlich sind nach § 6 Abs. 2 MDStV noch die verantwortlichen Personen für den journalistischen Text mit Namen und Anschrift zu benennen. Empfehlenswert ist darüber hinaus die Angabe von Telefon- und Telefaxnummer, die eine Kontaktaufnahme erleichtern. Erfolgt die technische Abwicklung des Angebots durch ein Rechenzentrum des Schulträgers oder andere Dritte, so sind diese dann in der Anbieterkennzeichnung ebenfalls aufzuführen.

Während der Inhalt der Anbieterkennzeichnung zwar unmissverständlich normiert ist, fehlt es jedoch an einer Regelung der Präsentation. Sie ergibt sich allerdings aus dem Zweck der Anbieterkennzeichnung. Die Anbieterkennzeichnung ist so zu platzieren und auszugestalten, dass sie leicht auffindbar und gut lesbar ist.

Die Anbieterkennzeichnung hat zumindest auf einer Seite der Homepage die vollständigen Angaben zu enthalten. Beim Aufrufen der Homepage sollte auf jeden Fall eine eindeutige Kurzbezeichnung (der Anbieterkennzeichnungsanker) und eine direkte Verweisung (Link) auf die vollständige Anbieterkennzeichnung vorhanden sein ("one click away"). Da im Internet nicht immer ein Einstieg über die Startseite der Homepage notwendig ist, ist zusätzlich zu gewährleisten, dass die Nutzer/innen auch von allen übrigen Seiten der Homepage direkt auf diejenige Seite gelangen können, von der aus auf die Anbieterkennzeichnung zugegriffen werden kann ("two clicks away"). Der Anbieterkennzeichnungsanker sollte ohne Schwierigkeiten gefunden werden können. Dabei sollte eine bekannte und als solche eindeutig erkennbare Anbieterkurzbezeichnung gewählt werden. Auch farblich sowie hinsichtlich der Schriftart und -größe sollte eine gute Erkennbarkeit und Lesbarkeit sichergestellt werden. Daher ist es empfehlenswert, dass starke Kontraste in Farbe und Linienführung gewählt werden. Die Anbieterkennzeichnung ist so auszugestalten, dass sie problemfrei auszudrucken ist.

### 4.2.2 Anzeige der Weitervermittlung

Eine Weitervermittlung an Dritte – etwa zu Homepages anderer Schulen – mittels eines Link ist nach § 4 Abs. 3 TDDSG, § 13 Abs. 3 MDStV anzuzeigen. Auch hier steht der Gedanke der Transparenz im Vordergrund. Der Anzeige der Weitervermittlung kann beispielsweise durch einen unmissverständlichen Hinweis in Wortform Genüge getan werden oder durch Schaltung einer Zwischenseite, die auf die vermittelte Adresse hinweist und den Abbruch der Weiterschaltung ermöglicht. Auch sollte jederzeit erkennbar sein, wer für die aufgerufene Seite verantwortlich ist. Es kann irreführend sein, wenn zum Beispiel der Rahmen (Frame) der Homepage einer Schule bei einer nicht erkennbaren Weitervermittlung noch vorhanden ist. Unter Umständen sind dann die Anbieter/innen der Homepage nach § 5 TDG und § 5 MDStV auch für den fremden Inhalt der/des Dritten verantwortlich.

### 4.2.3 Unterrichtungspflichten

Damit Angebote für die Nutzer/innen schnell und unkompliziert abzurufen sind, werden oft so genannte Cookies verwendet. Cookies sind Datensätze, die von Internetservern auf die Rechner der Nutzer/innen übermittelt werden und dort in einer Datei auf der Festplatte abgelegt werden. Mit Hilfe von Cookies können Informationen über die Verweildauer auf bestimmten Seiten, die Häufigkeit des Seitenaufrufs und dergleichen mehr ermittelt werden. Cookies dürfen – soweit sie personenbeziehbare Angaben ermitteln – nur mit Einwilligung der Nutzer/innen gesetzt werden. Nach § 3 Abs. 5 Satz 1 TDDSG, § 12 Abs. 6 Satz 1 MDStV sind die Nutzer/innen vor Erhebung, Verarbeitung und Nutzung ihrer personenbezogenen Daten zu unterrichten. Da bei Cookies die Verarbeitung personenbezogener Daten erst zu einem späteren Zeitpunkt als dem ersten Aufruf der Seite erfolgt, verlangt § 3 Abs. 5 Satz 2 TDDSG, dass die Nutzer/innen vor Beginn des automatisierten Verfahrens, welches eine spätere Identifizierung der betroffenen Person ermöglicht und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereitet, zu informieren sind.

Auch Programme wie Active-X, JavaScript oder Plug-Ins können ebenso wie Cookies eine Nutzeridentifikation ermöglichen. Hier gelten die bereits im Zusammenhang mit Cookies beschriebenen Anforderungen. Die genannten Programme stellen zusätzlich eine große Sicherheitsgefahr dar, da sie den

Nutzerrechner bei unzureichender Sicherheitseinstellung ausspähen können. Des weiteren können diese Programme Viren enthalten und sie auf dem Nutzerrechner ablegen.

### 4.2.4 Transparenz durch Datenschutzpolicies

Wer es mit dem Selbstbestimmungsrecht seiner Nutzer/innen ernst meint, sollte darüber hinaus Datenschutzhinweise (Datenschutzpolicy) an gut lesbarer Stelle geben. Damit wird offen gelegt, wie mit automatisch anfallenden Daten – den Spuren im Netz – umgegangen wird und ob Cookies oder aktive Inhalte verwendet werden. Sollen personenbezogene Daten erhoben werden, ist das nur aufgrund einer dies ausdrücklich erlaubenden Rechtsvorschrift zulässig oder wenn eine wirksame Einwilligung erteilt ist. Auch wenn keine personenbezogenen Daten bei den Nutzer/innen erhoben werden, wird bei jeder Internetnutzung auf der Homepage zwangsläufig die IP-Adresse der Kommunikationsverbindung bekannt. Zwar ist es nicht so, dass diese Adresse immer personenbeziehbar ist, da im Regelfall Nutzer/innen über Accessprovider dynamische IP-Adressen zugeordnet werden. Aus Gründen der Transparenz empfiehlt es sich jedoch, darauf hinzuweisen, in welcher Form welche Datensätze gespeichert werden. Und schließlich rundet der Hinweis, dass auf Cookies und aktive Programme verzichtet wird, die Datenschutzpolicy ab.

**Inhalt einer Datenschutzpolicy:**
Mit dem Zugriff auf die Web-Site werden die um die letzte Stelle der letzten Zahl verkürzte IP-Adresse und weitere Angaben (Datum, Uhrzeit, letzte betrachtete Seite) auf dem Internetserver zu Zwecken der Datensicherheit und statistischen Zwecken eine bestimmte Zeit lang (Angabe der Zeitdauer) gespeichert. Durch die Verkürzung der IP-Adresse ist ein Bezug der gespeicherten Daten zu Ihnen ausgeschlossen. Auf die Verwendung von Cookies und aktive Inhalte wird verzichtet.

### 4.2.5 Individuelle Informationspflichten – elektronische Auskunft

Das Recht, wissen zu können, wer was über die eigene Person weiß, hat insofern seinen Niederschlag gefunden, als § 7 TDDSG und § 16 Abs. 1 MDStV das Auskunftsrecht jeder Nutzerin und jedes Nutzers über die zur eigenen Person oder auch zum Pseudonym gespeicherten Daten normiert. Die Betroffenen müssen die Unterlagen einsehen oder auf Wunsch auch elektronische Auskunft erhalten können.

## 5 Technische Absicherung

Der Anschluss an das Internet ist mit erheblichen Gefährdungen der Datensicherheit und des Datenschutzes verbunden. Jeder muss damit rechnen, beim Surfen beobachtet zu werden. Es wird erfasst, wer (welcher PC) das Internet wie nutzt, welche Seiten aufgerufen werden und wie lange. Diese Angaben reichen zwar noch nicht aus, um zu erkennen, wer den PC gerade nutzt. Eine Zuordnung ist aber unter Umständen später möglich, wenn bei anderer Nutzung die Identität der Nutzerin des oder Nutzers selbst preisgegeben wird. Weiter sind die Knotenrechner und die Übertragungswege dieses weltweiten Netzes nicht bekannt. Welchen Weg eine E-Mail nimmt oder in welchem Vermittlungsrechner die Nachricht bearbeitet wird, ist nicht vorher bestimmbar. Im Internet wird grundsätzlich den Risiken für Vertraulichkeit, Integrität und Zurechenbarkeit nicht in der gebotenen Weise begegnet. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Rechnersystemen. Ohne besondere Schutzmaßnahmen können sich Angreifer/innen oft mit wenig Aufwand unter Aus-

nutzung der Sicherheitslücken unberechtigten Zugang zu fremden Rechnern verschaffen und dort Daten ausspähen, manipulieren oder zerstören. Dies ist besonders gravierend, weil angesichts von ca. 200 Millionen Internet-Teilnehmer/innen auch die Zahl der potentiellen Angreifer/innen, die diese Sicherheitslücken ausnützen, signifikant ist.

**Diesem Risiko müssen die Schulen Rechnung tragen; dazu verpflichtet sie § 7 NDSG.**

Diese Pflicht kann bei einem Internet-Anschluss am besten und sichersten durch eine sogenannte Insellösung, also den Verzicht auf Vernetzung des Verwaltungsrechners der Schule mit den Rechnern, die ans Internet angeschlossen sind, realisiert werden. Es empfiehlt sich in jedem Falle eine strikte Trennung zwischen der für die Schulverwaltung notwendigen Verarbeitung von personenbezogenen Daten und dem Internet-Zugang. Web-Server sollten sich auf jeden Fall außerhalb der lokalen Netze der Schulen befinden. Die auf dem Web-Server gespeicherten Daten – das sind sowohl solche, die sich aus dem Web-Angebot selbst ergeben, als auch solche, die im Rahmen des normalen Unterrichts anfallen – sind durch geeignete Maßnahmen gegen unbefugten Zugriff zu sichern.

Bei einem Zugang aus dem lokalen Netz der Schule in das Internet sowie zur Online-Pflege des Web-Servers, empfiehlt sich der Einsatz einer Firewall zwischen dem lokalen Netz und dem Web-Server. Zusätzlich sollte der Web-Server selbst gegen Manipulationen aus dem Internet geschützt werden. Grundsätzlich sollten nur die unbedingt erforderlichen Dienste und Protokolle aktiviert sein, die Schreibrechte sollten auf das unabdingbare Maß beschränkt werden und eine Anzeige der Verzeichnisstruktur nicht möglich sein. Weitere Informationen zum Aufbau und zur Installation einer gesicherten Serverumgebung sind in der Orientierungshilfe „Datenschutz bei der Nutzung von Internet und Intranet“ des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder zu finden; erhältlich als Druckausgabe beim LfD. Beim Betreiben eigener Webserver sollte darüber hinaus auf Folgendes geachtet werden:

- Der direkte Zugriff auf Datenbanken der Schule sollte grundsätzlich verhindert werden. Soweit ein Datenbankzugriff erforderlich ist, sollten Kopien verwendet werden.
- Das Internet-Angebot ist durch geeignete Maßnahmen gegen unbefugte Manipulationen zu sichern. Hierzu gehören eine sichere Konfiguration der Rechteverwaltung und eine geeignete Protokollierung unerlaubter Zugriffe auf dem Webserver.
- Besonderes Augenmerk ist auf personenbezogene Daten zu richten, die durch die Nutzung entstehen. Sie müssen gegen den Zugriff über das Internet geschützt werden und sollten nur kurzfristig im Web-Server gespeichert sein.

Zusätzlich zur Firewall müssen Maßnahmen gegen schädliche Kommunikationsinhalte, wie z.B. Computerviren, ActiveX- und Java-Programme sowie sonstige aktive Inhalte von Webseiten, getroffen werden. Informationen hierzu können der Orientierungshilfe **„Internet“** des AK Technik der LfD-Konferenz unter www.datenschutz.de und den Orientierungshilfen und Selbstschutz-Checklisten unter www.lfd.niedersachsen.de entnommen werden.

# 6 Nutzungsordnung

## 6.1 Ziel und möglicher Weg einer Regelung

Für die schulische Internet-Welt sind verbindliche Regeln erforderlich, die insbesondere Nutzungsumfang, Art und Weise der Nutzung und die Kontrolle von Missbrauch festlegen. Wie ein solches Regelwerk ausgestaltet wird, ist – im Rahmen der verbindlichen gesetzlichen Vorgaben – im Wesentlichen die Angelegenheit jeder einzelnen Schule. Die Schule hat die Möglichkeit, eine auf ihre Bedürfnisse zugeschnittene Nutzungsordnung als eigene Schulordnung zu erlassen.

Um etwaigen Missverständnissen vorzubeugen, sei betont: Vorschriften einer Nutzungsordnung vermögen nicht die individuelle Einwilligung in die Verarbeitung personenbezogener Daten zu ersetzen, soweit diese erforderlich ist.

## 6.2 Gegenstand und Elemente

Auch wenn inzwischen viele Schulen über einen Internet-Zugang verfügen, ist die Ausstattung noch sehr unterschiedlich. In manchen Schulen ist nur ein Internet-PC im Lehrerzimmer aufgestellt, andere verfügen bereits über vernetzte Multimedia-Arbeitsplätze in den Klassenzimmern oder sogenannte Medienecken, die den Zugang zum Netz auch unabhängig vom Unterricht ermöglichen. Ziel, Art und Umfang des angestrebten Internet-Einsatzes werden beispielsweise auch nach Schultyp und Alter der Schüler/innen differieren. In einer Nutzungsordnung sollte insbesondere Folgendes geregelt werden:

- Wer ist für die Systemadministration verantwortlich?

- Welche Internetdienste werden an der Schule zugelassen und welche Nutzungsrechte sollen Lehrkräfte, Schüler/innen und gegebenenfalls auch die Erziehungsberechtigten haben? Hierzu gehört neben der Festlegung der zugangsberechtigten Personengruppen, der zulässigen Nutzungsarten und des Nutzungsumfangs auch eine Regelung der Vergabe der Nutzungsrechte, deren Kriterien und der Verwaltung der Nutzungsberechtigungen.

- In welchem Rahmen und Maß sollen die Lehrkräfte weisungsbefugt sein? Diesbezüglich ist vor allem zwischen der Nutzung des Internets inner- und außerhalb des Unterrichts zu unterscheiden.

- Welche Lehrkraft ist für die Homepage verantwortlich? Soll die Veröffentlichung eines Beitrags von Schüler/innen (mit Ausnahme der Schülerzeitung) genehmigungspflichtig sein?

- Welche Daten dürfen zu welchem Zweck im Rahmen schul- oder unterrichtsbezogener Internetnetzungen protokolliert werden, wer darf die Protokolldatei einsehen, auf Verlaufsdateien oder andere temporäre Internet-Dateien zugreifen und wann sind die Protokolldaten von wem zu löschen?

- Welche Verstöße gegen Nutzungsregeln werden mit welchen Maßnahmen geahndet und welche Kontrollen werden in diesem Zusammenhang von wem durchgeführt? Außerdem sollte über die Verfahrensweise bei strafrechtlich relevantem Beschaffen oder Verbreiten von Informationen belehrt (Anzeige), insbesondere aber auch die schulischen Konsequenzen für die Nutzer/innen festgelegt werden (Löschung der Nachricht, Sperrung der oder Ausschluss von der Nutzung).

Einem höheren Maß an Klarheit könnte es dienen, in die Nutzungsordnung auch (deklaratorische)

Hinweise auf medienrechtliche Bestimmungen und deren datenschutzrechtliche Grundsätze aufzunehmen – etwa dass das Fernmeldegeheimnis zu beachten ist und dass Kontrollen zur Feststellung von unerlaubten Nutzungen außerhalb des Unterrichts nur mit Kenntnis der Betroffenen und nur bei konkreten Anhaltspunkten oder stichprobenartig durchgeführt werden dürfen.

# 7 Begriffserklärungen

**Account** Account heißt übersetzt Konto. Gemeint ist ganz allgemein der Zugang zum Internet oder sonstigen Netzen. Ein Account beinhaltet immer einen Usernamen, ein Passwort und natürlich bestimmte Nutzungsbedingungen.

**Active-X, Java, JavaScript, Plug-Ins** Active-X-Controls, Java-Applets und JavaScripts sind Programme, die beim Aufrufen von Angeboten auf den Rechner des Nutzers heruntergeladen und dort zur Ausführung gebracht werden. Eine Gefahr geht insbesondere von Programm-Einheiten aus, die unter Ausnutzung von Sicherheitslücken Funktionen mit schädlichen Eigenschaften beinhalten. Diesen Gefahren kann der Nutzer durch Deaktivierung der Ausführbarkeit der Programme begegnen. Anbieter sollten daher damit rechnen, dass Nutzer beispielsweise Active-X-Controls, Java-Applets oder Plug-Ins (im Nutzerbrowser installierte Zusatztools) nicht ausführen können. Dies gilt insbesondere für Active X-Programme, von denen im Allgemeinen die weitreichendsten Gefährdungen für Internet-Nutzer ausgehen. Die Informationsangebote sollten dementsprechend ohne solche Programme gestaltet werden.

**Archie** Archie ist ein mächtiger Dienst für die weltweite Suche nach Dateien auf IMG SRC="../../gif/pfeil.gif"> FTP-Servern. Der Zugriff erfolgt über Telnet, E-Mail oder einen eigenen Archie-Client. Als Suchergebnis liefert Archie entweder Server-, Verzeichnis- und Dateinamen oder eine Kurzbeschreibung zu gesuchten Dateien.

**Attachment** Heute kann man an E-Mails Dateien (z. B. ein Winword-Dokument) anhängen und gemeinsam verschicken. Diese Anlagen werden Attachments genannt.

**Brett** Brett ist die deutsche Bezeichnung für Newsgroup. Der Begriff ist vor allem in Mailboxnetzen geläufig und kommt von dem Vergleich mit einem schwarzen Brett, einer Pinwand für öffentliche Nachrichten. Newsgroups werden auch Foren oder Diskussionsgruppen genannt.

**Browser** Ein Browser ist das Programm, mit dem man durch das WWW surfen kann. Ein Browser ist notwendig, um WWW-Seiten überhaupt anschauen zu können (siehe auch HTML).

**Cookies** Cookies (engl. cookie = Keks) sind kleine Datenmengen, die zusammen mit den eigentlich angeforderten Daten aus dem Internet an den Computer des Benutzers übermittelt werden. Dort werden diese Daten gespeichert und für einen späteren Abruf bereitgehalten. Dadurch wird im einfachsten Fall ein wiederholter Zugriff eines bestimmten Benutzers (exakt: des Browsers auf dem Computer, den er verwendet) auf das Internet-Angebot erkennbar. Vor allem Firmen benützen Cookies, um Kundenprofile zu erstellen, oder ein persönliches Angebot zusammenstellen zu können. Man kann einstellen, ob der Browser Cookies akzeptieren darf: InternetExplorer 4.0: Menü Ansicht/Optionen/ Erweitert, Netscape 4.0: Menü Bearbeiten/Einstellungen/Erweitert.

**DFÜ** DFÜ (Abk. für Datenfernübertragung) ist der Sammelbegriff für alles, was elektronische Kommunikation beinhaltet, besonders verbreitet im Mailboxbereich.

**Domain** Eine Domain ist eine weltweit erreichbare Adresse, die von Computern im Internet gebraucht wird, um Nachrichten automatisch zustellen zu können. Rheinmain.de, spiegel.de oder aol.com sind z. B. eine Domain, siehe auch Username.

**Download** Download nennt man den Vorgang, wenn man sich von einem fremden Rechner via DFÜ eine Datei lädt. Man stellt sich den fremden Rechner quasi oben und den eigenen unten vor (siehe auch Upload).

**E-Mail** Electronic Mail (kurz E-Mail) ist der am weitesten verbreitete Internet-Dienst. E-Mail ermöglicht das Verschicken von „elektronischen Briefen“ zwischen mehreren Computerbenutzern. Die Nachrichten können aus Texten, Programmen, Grafiken oder Tönen bestehen. Sender und Empfänger müssen jeweils eine eindeutige E-Mail-Adresse besitzen (Form: Name@Anschrift), die ähnlich der postalischen Anschrift funktioniert. Um E-Mails in andere Datennetze zu verschicken oder von dort zu empfangen, werden Gateways benötigt, die den Übergang von einem System zum anderen handhaben. E-Mail kann außerdem für eine indirekte Inanspruchnahme von anderen Diensten (z. B. FTP, WWW) genutzt werden. Mailbox.

**Emoticons** Auch Smileys genannt, mit ihnen werden Stimmungen in Texten (z. B. in mail und news) ausgedrückt (z. B.: **:-)** lächeln; **;-)** verschmitzt lächeln;
:-(traurig).

**FAQ** FAQs (Abk. für Frequently Asked Questions) sind sehr hilfreiche Texte, die für Neueinsteigerinnen und Neueinsteiger empfehlenswert sind und verhindern sollen, daß immer dieselben Fragen gestellt werden.

**Finger** Finger ist ein Werkzeug zur Suche nach Informationen über Personen und Rechner, die an der Kommunikation im Internet beteiligt sind. Es können sowohl personenbezogene Daten (Name, E-Mail-Adresse, Telefonnummer, Arbeitszeit, öffentliche Schlüssel usw.) als auch sicherheitsrelevante Informationen über angeschlossene Rechner in Erfahrung gebracht werden.

**FTP** FTP steht für File Transfer Protocol und dient dem Übertragen von Dateien zwischen Rechnern mit Hilfe eines normierten Befehlssatzes. Auf dem eigenen Rechner läuft der FTP-Client, der die Befehle an den entfernten FTP-Server weiterleitet. Voraussetzung für die Nutzung sind Accounts auf beiden Rechnern oder eine öffentliche Zugriffsmöglichkeit auf dem FTP-Server durch „Anonymous FTP“, wodurch ein eingeschränkter Zugriff auf bestimmte Dateien des entfernten Rechners ermöglicht werden kann. Weltweit gibt es tausende Anonymous-FTP-Server, die Programme, Texte, Grafiken oder Tondateien bereithalten.

**Gate(way)** Ein Gateway ist ein Computer, der den Übergang von einem Netz zu dem anderen (z. B. von dem Internet zu einem Mailboxnetz) darstellt. Gateways sind notwendig, da die verschiedenen Netze mit unterschiedlichen technischen Sprachen ( Protokollen) arbeiten.

**Gopher** Gopher ist ein Menü-orientiertes Werkzeug zur Recherche, das unabhängig davon eingesetzt werden kann, auf welchem Rechner die gesuchten Informationen zu finden sind, in welchem Format sie vorliegen und welche Zugriffsmöglichkei-

zu finden sind, in welchem Format sie vorliegen und welche Zugriffsmöglichkeiten ( FTP, Telnet, WAIS usw.) existieren. Jeder Gopher-Server ist öffentlich zugänglich. Benutzer können mit ihrem Gopher-Client nur lesend auf die angebotenen Daten zugreifen. Gopher ist im WWW integriert.

**Header** Der Header ist der erste Teil (Vorspann) einer Nachricht, in dem die Adresse, der Absender, die Länge der Nachricht, das Datum und andere Informationen stehen.

**HTML** HTML (Abk. für Hypertext Markup Language) ist die Sprache, in der Webseiten geschrieben werden. Erst der Browser ermöglicht eine grafische Umsetzung der HTML Befehle. Das Besondere von HTML sind die universelle Einsetzbarkeit für alle Arten von Computern und die Verweise, sog. Links.

**HTTP** HTTP (Abk. für Hypertext Transport Protokoll) ist quasi die technische Grundlage für das WWW. Dem Computer wird mitgeteilt, dass die Daten aus HTML-Code bestehen, deswegen beginnen WWW Adressen mit http:// Bei neueren Browsern funktioniert das Ansehen von Webseiten allerdings auch, wenn man http:// weglässt.

**Hypertext** Hypertext wird ein Text genannt, der interaktive Verweise ( Links) beinhaltet.

**IRC** IRC (Internet Relay Chat) ist ein Internetdienst, der die Möglichkeit bietet, nicht nur via E-Mail und Newsgroups zeitversetzt zu diskutieren, sondern „live“ in Echtzeit rund um die Welt.

**ISDN** ISDN ist eine Telefon(leitungs)-Technik. Herkömmliche Telefonleitungen funktionieren analog, d. h. übertragen Töne. ISDN hingegen funktioniert – wie der Computer – digital und überträgt also 0 und 1. ISDN bedeutet vor allem auch dadurch eine Geschwindigkeitsverbesserung. Ein ISDN-Anschluss beinhaltet 3 bis 10 Rufnummern und 2 Leitungen, was den Nebeneffekt hat, dass man während des Surfens auch telefonieren kann.

**IP-Adresse, IP-Nummer** IP-Adressen sind Zahlenkombinationen wie z. B. 195.35.6.214. Diese Zahlenkombinationen sind die Adresse des Computers. Jeder Computer hat sowohl eine Adresse aus Wörtern (siehe Domain) als auch eine IP-Adresse. Die IP-Adresse wird von den Computern benutzt, die Namen sind für die Menschen leichter zu merken.

**Link** Link ist der engl. Ausdruck für Verbindung und bezeichnet die (anklickbaren) Verweise von einer WWW-Seite auf eine andere.

**Mailbox** Im Internet wird das Wort Mailbox für ein persönliches Postfach benützt, in dem eingehende Nachrichten ( E-Mails) gespeichert werden.

Ansonsten ist damit allerdings ein Mailbox-Computer gemeint, der anrufbar ist und nicht nur die persönliche Post für seine Nutzerinnen und Nutzer aufbewahrt, sondern auch öffentliche Diskussionsforen anbietet. Auch Firmen bieten manchmal Mailboxen an, um Produktinformationen, Treiber und Software anzubieten. Eine Mailbox muss man direkt anrufen (dazu muss man oft einen Account besitzen) und im Gegensatz zum Internetprovider verlässt man den angerufenen Rechner nicht, sondern greift nur auf dort vorhandene Informationen zu. Deswegen sind Mailboxen zu Mailboxnetzen zusammengeschlossen, um eine

Vielzahl von Informationen anbieten zu können

**Mailingliste** Eine Mailingliste ist eine Art Diskussionsforum via Briefverteiler. Alle teilnehmenden Personen müssen sich bei dem Mailinglistenverteiler anmelden und schicken alle Nachrichten dorthin. Die Nachrichten werden dann an alle Teilnehmerinnen und Teilnehmer weitergeleitet. Mailinglisten gibt es zu allen erdenklichen Themen. Je nach Mailingliste können verschiedene Regeln gelten. Generell stellt man sich meistens kurz vor. Mailinglisten bieten überschaubarere Gemeinschaften als Newsgroups.

**Metasearch** Metasearch nennt man eine Suche, die in mehreren Katalogen und Datenbanken unterschiedlicher Suchmaschinen gleichzeitig erfolgt, bzw. eine Suchmaschine, die anbietet, auf einfache Art und Weise dieselbe Suche auf beliebigen Suchmaschinen durchzuführen.

**Netcall** Netcall nennt man sowohl den Datenaustausch von Mailboxen untereinander als auch das Anrufen und Nachrichtenabgleichen eines Points bei der Mailbox.

**Netikette** Die Netikette ist die Menge der Umgangsregeln für das Internet und die anderen Netze.

**Newsgroup** Newsgroup ist die Internetbezeichnung für öffentliche Foren, Gesprächsgruppen, also den öffentlichen Bereich, in dem alle die von einer Person gesendeten Nachrichten lesen und beantworten können (siehe auch Usenet-News, Brett).

**Online** Online bedeutet „mit offener Telefonleitung“. Nach der Einwahl beim einem Provider oder einer Mailbox ist man „online“, also mit bestehender Telefonverbindung zu einem anderen Rechner.

**Offline** Offline ist das Gegenteil von Online. Aus Kostengründen gibt es auch Programme, mit denen man Nachrichten lesen und schreiben kann ohne Telefonverbindung und erst hinterher die fertigen Nachrichten über die Telefonleitung verschickt.

**PGP** Pretty Good Privacy, ein Verschlüsselungsprogramm für E-Mails. Das Programm kann sowohl elektronische Unterschriften leisten als auch E-Mails sicher verschlüsseln.

**Point** Ein Point ist ein Programm, dass sich in die Mailbox (2.) einwählt und automatisch die neuen Nachrichten empfängt und versendet, so dass man die Nachrichten in Ruhe daheim schreiben kann, ohne bestehende Telefonverbindung ( offline).

**PoP** PoP (Abk. für Point of Presence), gleichbedeutend mit Provider, bzw. Einwahlknoten.

**Postmaster** Postmaster sind die Verantwortlichen eines Systems. Bei Unis oder sonstigen Providern gibt es in der Regel immer einen Account Postmaster, an den man schreiben kann, wenn man Hilfe braucht.

**PPP** (Point to Point Protocoll) PPP ist notwendig, um sich von Zuhause über Modem und Telefonleitung ins Internet einzuwählen. Die meisten Betriebssysteme und Provider unterstützen dieses Protokoll.

**Protokoll** Ein Protokoll ist eine technische Regelung von Abläufen, quasi eine Sprachregelung, mit der sich Computer verständigen.

**Provider** Ein Provider ist ein Internetanbieter. Er ermöglicht Privatpersonen/Firmen Zugang zum Internet.

**Proxy** Ein Proxy-Server ist ein Rechner, der nicht direkt jede Anfrage einer Internetadresse in das Netz weitergibt, um die Seite anzufordern, sondern erst in seinen Speicher nachschaut, ob jemand diese Seite heute (oder in den letzen Stunden oder etc.) bereits aufgerufen hat, so dass er sie nicht erneut anfordern muss. Er speichert also jede angeschaute Datei zwischen, um so die Leitungen zu entlasten. Proxy-Server werden vor allem auch bei Firmenintranets, die ans Internet angeschlossen sind, verwendet, um Verbindungskosten zu sparen und die Arbeitsgeschwindigkeit zu erhöhen.

**Signatur(e)** Abspann nach einer Mail. Meist ein Spruch oder vielleicht auch eine Postadresse, die ähnlich wie bei einem bedruckten Briefpapier immer mitgeschickt wird. Es sollten nur kurze Signaturen verwendet werden, da lange Signaturen eine überflüssige Datenlast ausmachen, die die Leitungen belegt.

Digitale Signatur: Siegel zu digitalen Daten, das den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt (vgl. auch § 2 Abs. 1 Signaturgesetz). Ein solches Siegel wird mit Hilfe spezieller kryptographischer Verfahren aus dem Signaturschlüssel und den Daten erzeugt.

**TCP/IP** Internetprotokoll (genaugenommen zwei verschiedene Protokolle: Transmission Control Protocol/Internet Protocol). Die technische Erfindung, die es erlaubt, dass sich völlig unterschiedliche Computer verstehen können und die festlegt, was warum wie wohin gesendet wird und somit die technische Basis des Internets darstellt.

**Telnet** Mit Hilfe von Telnet ist es möglich, auf einem entfernten Rechner eine Terminalsitzung aufzubauen (Remote Login) und textorientierte Anwendungen zu nutzen. Dazu benötigt man einen Account oder einen öffentlichen Zugang auf dem entfernten Rechner. Über Telnet sind zum Beispiel Informationssysteme wie Datenbanken oder Bibliotheken zu nutzen (z. B. Archie). Telnet wird ebenfalls häufig für die Fernwartung von Rechnern eingesetzt.

**URL** Ein URL (Universal Ressource Locator) ist eine exakte Adressangabe für Dateien im Internet. `Http://tal.cs.tu-berlin.de/~babajaga/fliegen` ist ebenso eine URL wie `http://www.tagesschau.de`.

**Usenet-News** Öffentliche Nachrichten werden im Internet in thematisch gegliederten Diskussionsforen ( Newsgroups) ausgetauscht. Dieser News-Dienst wird auch als Usenet (Kurzform von Users´ Network) bezeichnet. Er gleicht einer riesigen Zeitung mit Fachartikeln, Leserbriefen und Kleinanzeigen. Zurzeit gibt es etwa 10.000 verschiedene Newsgroups, in denen pro Monat rund 3,2 Millionen Artikel mit einem Datenvolumen von ca. 14 GB geschrieben werden (Stand: August 1995). Die Artikel werden auf zentralen Rechnern (Newsservern) in Datenbanken gehalten; der Zugriff erfolgt über Newsreader-Programme.

**Username /** Name, der jeder Benutzerin und jedem Benutzer zugewiesen wird, z. B. `nora.b`

**User-ID** danach kommt immer ein @ und der Name der Mailbox oder des Heimatrechners (also des Providers z. B.) und danach die Domain (die Internetadresse des Rechners). Im Gesamten also `nora.b@ipn-b.de`[7] Der Teil der Adresse nach dem @ kann unterschiedlich lang sein und hängt von dem Heimatrechner bzw. Provider ab.

**Wais** WAIS (Wide Area Information Server) ermöglicht eine Volltextsuche in einer Vielzahl von Datenbanken ohne Kenntnis komplizierter Abfragesprachen. WAIS-Abfragen können mit Telnet, E-Mail, einem eigenen WAIS-Client oder über WWW durchgeführt werden.

**WhoIs** WhoIs wurde speziell zur Recherche nach personenbezogenen Daten von im Internet registrierten Nutzerinnen und Nutzern entwickelt. Das Vorhaben, eine Datenbank mit weltweit allen Internet-Nutzern aufzubauen, konnte nicht realisiert werden. Zurzeit existiert eine Vielzahl von einzelnen WhoIs-Servern, auf die mit Telnet oder mit besonderer Client-Software zugegriffen werden kann.

**www** Der Internet-Dienst WWW (World Wide Web) kann nahezu alle anderen Dienste integrieren. Durch einen multimediafähigen Hypertext-Mechanismus wird eine einfache Bedienbarkeit erreicht. Der Kommunikation zwischen dem WWW-Client und dem WWW-Server, der die multimedialen Daten anbietet, liegt das Protokoll HTTP (HyperText Transport Protocol) zugrunde. Die WWW-Dokumente werden mit der Definitionssprache HTML (HyperText Markup Language) erstellt. Für die Generierung interaktiver WWW-Seiten können CGI (Common Gateway Interface)-Skripte installiert werden.

## 8 Abkürzungsverzeichnis

| | |
|---|---|
| ARP | Address Resolution Protocol |
| BDSG | Bundesdatenschutzgesetz |
| CGI | Common Gateway Interface |
| DMZ | Demilitarisierte Zone |
| DNS | Dynamic Name Service |
| FTP | File Transfer Protocol |
| HTML | HyperText Markup Language |
| HTTP | HyperText Transport Protocol |
| ICMP | Internet Control Message Protocols |
| IP | Internet Protocoll |
| MDStV | Mediendienste-Staatsvertrag |
| NBG | Niedersächsisches Beamtengesetz |
| NDSG | Niedersächsisches Datenschutzgesetz |
| NFS | Network File System |
| SSH | secure shell |
| TCP | Transmission Control Protocol |
| TDDSG | Teledienstedatenschutzgesetz |
| TDG | Teledienstegesetz |
| TKG | Telekommunikationsgesetz |
| WWW | Word wideWeb |

## 9 Wichtige Links

Jeder Internet-Nutzer sollte sich mit Fragen der Sicherheit im Internet befassen. Es gibt inzwischen eine ganze Reihe von technischen Möglichkeiten, sich selbst zu schützen. Selbstdatenschutz ist für jeden sicherheitsbewussten Internetnutzer erforderlich und möglich. Die Datenschutzbeauftragten geben Ihnen hierzu gern Hinweise und Tipps. Hier sind einige interessante Web-Adressen:

| | |
|---|---|
| **www.lfd.niedersachsen.de** | Bietet einen kostenlosen Selbsttest für Ihren Internet-PC an und enthält Checklisten zum sicheren Internetanschluss. |
| **www.datenschutz.ch** | Bietet einen ähnlichen Browser-Test an. |
| **www.datenschutz.de** | Enthält Tipps zum anonymen Surfen und bietet Diskussionsforen für Interessierte an. |
| **www.sicherheit-im-internet.de** | Hat aktuelle News zu Sicherheits-Produkten und gibt praktische Einführungen in Sicherheits-Tools. |
| **www.bsi.de** | Bietet vertiefende Ausführungen zum Thema „Informationssicherheit“. |