

# „Schulen ans Netz“

## Inhaltsverzeichnis

- Stand 10.04.2001 -

### 1. Einführung

### 2. Technische Absicherung

### 3. Internet im Unterricht

#### 3.1 Gegenstand des Unterrichts

##### 3.1.1 Datenschutz und (Selbst-)Verantwortung

##### 3.1.2 Risiken der Internetnutzung

##### 3.1.3 Schutzmaßnahmen

#### 3.2 Nutzung im Unterricht

### 4. Internetnutzung außerhalb des Unterrichts in der Schule

#### 4.1 Grundsatzentscheidung und Verantwortlichkeit

#### 4.2 Zugangskontrollen

### 5. Homepage

#### 5.1 Inhaltsdaten: Was darf ins Internet?

##### 5.1.1 Grundsätzliches

##### 5.1.2 Daten von Lehrer/innen

##### 5.1.3 Daten von Schüler/innen und Erziehungsberechtigten

##### 5.1.4 Gästebuch, schwarzes Brett und Kontaktlisten

##### 5.1.5 Beiträge von Schüler/innen

##### 5.1.6 Webcams

#### 5.2 Informationspflichten als Anbieterin

### 6. Nutzungsordnung

#### 6.1 Ziel und möglicher Weg einer Regelung

#### 6.2 Gegenstand und Elemente

## 1. Einführung

„Wir sind drin“ – alle nordrhein-westfälischen Schulen verfügen inzwischen über einen Internetzugang und mindestens einen angeschlossenen Multimedia-PC. Bis Ende 2004 sollen alle Klassen mit Computern ausgestattet und so der flächendeckende Einsatz im Unterricht gewährleistet sein.

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 allerdings oft erst gestellt, wenn es zu spät ist oder ganz offensichtlich etwas schief läuft: 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 16jährigen 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, die die Nutzung des Internets auch und gerade in der Schule bietet, sind unbestritten. Wie die genannten Beispielsfälle zeigen, sollten sich alle Beteiligten aber auch - und zwar noch vor dem Online-Start - der Risiken des Surfens, Chattens und Mailens im Netz bewusst sein und diesen durch entsprechende Sicherheitsmaßnahmen Rechnung tragen. Jede Schule sollte zudem vorab verbindliche Regeln festlegen, damit alle Beteiligten wissen, wer das Internet in der Schule wann und wie nutzen darf, welche Kontrollen und 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. Viel erreicht wäre einstweilen, wenn die folgenden Seiten dazu beitragen könnten, unnötige Crashes auf der Schul-Datenautobahn zu verhindern.

## 2. Technische Absicherung

Der Anschluss an das Internet ist mit erheblichen Gefährdungen der Datensicherheit und des Datenschutzes verbunden. Die Rechner und Übertragungswege dieses weltweiten Computernetzes sind nicht kontrollierbar. Welchen Weg eine Nachricht nimmt oder in welchem Vermittlungsrechner die Nachricht bearbeitet wird, ist nicht festgelegt. Es wird den Risiken für Vertraulichkeit, Integrität und Zurechenbarkeit vielfach 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 Ausnutzung der Sicherheitslücken unberech-

tigten 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. So ist nach Maßgabe des § 2 Abs. 1 der Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Erziehungsberechtigten (VO-DV I) eine **strikte Trennung** zwischen der ausschließlich für die Verwaltung notwendigen Verarbeitung von personenbezogenen Daten und dem Internet-Zugang erforderlich. Entsprechendes gilt auch hinsichtlich der Verarbeitung der Daten der Lehrkräfte nach § 2 Abs. 1 der Verordnung über die zur Verarbeitung zugelassenen Daten der Lehrerinnen und Lehrer (VO-DV II). Web-Server sollten sich deshalb auf jeden Fall außerhalb der lokalen Netze der Schulen befinden. Dies kann am besten und sichersten durch eine sogenannte **Insellösung**, also den Verzicht auf die Vernetzung des Verwaltungsrechners der Schule mit den Ausbildungsrechnern, die ans Internet angeschlossen sind, realisiert werden.

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. Besonderes Augenmerk ist auf die personenbezogenen 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.

Unabhängig hiervon muss den Risiken begegnet werden, denen die Lehrer/innen und Schüler/innen bei der Nutzung des Internets in der Schule ausgesetzt sind. Es müssen zum Beispiel Maßnahmen gegen Computerviren, schädliche ActiveX- und Java-Programme, fehlerhafte Bedienungen usw. getroffen werden.

Die Schule ist nach Maßgabe des § 10 Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) verpflichtet, die Einhaltung schulrechtlicher Bestimmungen über den Datenschutz sowie der Vorschriften des DSG NRW durch technische und organisatorische Maßnahmen sicherzustellen und diese Maßnahmen in einem **Sicherheitskonzept** zu dokumentieren.

### 3. Internet im Unterricht

#### 3.1 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 10jährigen 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 Gesichtspunkten 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:

### 3.1.1 Datenschutz und (Selbst-)Verantwortung

Nutzer/innen, die im Internet ihre personenbezogene Daten preisgeben, riskieren, dass Dritte diese Daten unzulässig nutzen. Ohne gesetzliche Grundlage oder wirksame Einwilligung dürfen Daten anderer Personen nicht verarbeitet 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, müssen sie zusätzlich medienrechtlichen Verpflichtungen genügen.

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 bestimmbarer 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? (Vgl. hierzu unter 5.1.1) 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.nrw.de](http://www.lfd.nrw.de) befindet.

### 3.1.2 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 abrechnungstechnischen Gründen bis heute grundsätzlich fremd. In aller Regel wird es personenbezogen, personenbeziehbar – über die sogenannte 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-, veränder- 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.

Abschließend ein **Tipp**: Am Beispiel der (unsicheren) E-Mail, die auf ihrem Weg durch das weltweite Internet viele Stationen passieren muss, in 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. Eine ausführliche (auch grafische) Darstellung ist zu finden unter [www.lfd.nrw.de/15. Datenschutzbericht/2.1.4.1 E-Mails](http://www.lfd.nrw.de/15_Datenschutzbericht/2.1.4.1_E-Mails) sowie unter [www.lfd.nrw.de/Info-Materialien/E-Mails ... aber sicher!](http://www.lfd.nrw.de/Info-Materialien/E-Mails...aber_sicher!).

### 3.1.3 Schutzmaßnahmen

Schließlich ist es 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 Geburtsdatum gefragt werden. Denn mit solchen Informationen werden unter Umständen zielgruppengerecht Werbungsmaterialien ausgesucht und übersandt. Die Federal Trade Commission, USA, hat Empfehlungen zusammengestellt, die unter [www.ftc.gov/bcp/online/edcams/kidzprivacy/index.html](http://www.ftc.gov/bcp/online/edcams/kidzprivacy/index.html) zu finden sind.

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, vgl. oben. Bei der Teilnahme an Foren und Chats aller Art, aber auch zum Surfen im Internet ist die Verwendung eines Pseudonyms nützlich.

Für die tägliche Schulpraxis gilt: In der Regel sollten Schüler/innen sowie Lehrer/innen ihre personenbezogenen Daten im Internet nicht preisgeben. Auch wenn bei einem Internet-Zugang über einen Schul-PC die individuelle Nutzung nach draußen meist ohnehin anonym bleibt, da in aller Regel nur die Kennung des Schul-PC in Erscheinung tritt, schadet die Verwendung eines Pseudonyms – etwa in Chatrooms – nicht. Ebenso sollten Nachrichten verschlüsselt werden, wenn ihr Inhalt niemand etwas angeht.

### 3.2 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 Partnerschule in Frankreich Kontakt via E-Mail pflegen und im Kunstunterricht virtuell durch die Uffizien spazieren. Eine Grundschule hat bereits eine Webcam in einem selbstgebauten Vogel-Nistkasten installiert, ein Gymnasium einen Öko-Atlas für die unmittelbare Schulumgebung erarbeitet und ins Netz gestellt.

Grundsätzlich ist die Nutzung aller schulintern erlaubten Internetdienste im Rahmen des Unterrichts zulässig; maßgeblich sind im konkreten Fall allerdings die Anweisungen der unterrichtenden Lehrkraft, die für die Schüler/innen verbindlich sind. Die Lehrer/innen dürfen die Einhaltung ihrer Anweisungen 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 generelle 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 ausnahmsweise und mit wirksamer Einwilligung der Betroffenen können auch 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 indes unverhältnismäßig. Eine Kontrolle sollte nur erfolgen, wenn dafür ein Anlass gegeben ist. In der ersten Stufe könnte eine stichprobenartige und nicht auf einzelne Nutzer/innen bezogene Auswertung der häufig angesurften Internet-Angebote erfolgen. Eine Auswertung der Protokolldateien könnte etwa daraufhin vorgenommen werden, welche Seiten ohne Bezug auf Unterricht oder Schule besonders häufig besucht werden. Ergeben sich dabei Zugriffe in signifikantem Umfang, sollten die Beteiligten zunächst pauschal auf die Unzulässigkeit dieses Verhaltens hingewiesen werden. Gleichzeitig sollte in Aussicht gestellt werden, dass bei Fortdauer der Verstöße eine personalisierte Kontrolle stattfindet. Fördert eine spätere Stichprobe tatsächlich weitere Zuwiderhandlungen gegen die Vorgabe zutage, kann festgestellt werden, von welchem Rechner aus unter welchem Account zu welcher Zeit solche Zugriffe stattgefunden haben.

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

## **4. Internetnutzung außerhalb des Unterrichts in der Schule**

Immer mehr Lehrer/innen und Schüler/innen möchten in der Schule auch nach Unterrichtschluss 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.

### **4.1 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, sollte jedoch vorab auf jeden Fall grundlegend diskutiert, sorgfältig abgewogen und in der Nutzungsordnung der Schule festgeschrieben werden, da sie weitreichende rechtliche Folgen auslöst. Hierbei ist zwischen verschiedenen Internetdiensten zu unterscheiden.

Wenn die Schule eine Telekommunikationsanlage (Vermittlungsserver) für die Kommunikation innerhalb der Schule und mit Dritten außerhalb der Schule betreibt, muss sie entscheiden, ob sie die Telekommunikationsdienste auch für private Zwecke erbringen will.

Relevant wird dies insbesondere für die Frage, ob die Schule Lehrer/innen und Schüler/innen den privaten **E-Mail-Verkehr** gestatten möchte.

Die Schule darf aus Sicherheitsgründen alle ein- und ausgehenden E-Mails auf Virenbefall kontrollieren, wenn die Kontrolle automatisch erfolgt. Dürfen die Vorgesetzten aber auf die an die Lehrer/innen gerichteten E-Mails auch inhaltlich zugreifen und diese lesen? Dürfen sie kontrollieren, wer eine Nachricht an wen versendet oder von wem bekommt? Die Antworten sind davon abhängig, ob es sich um eine private oder dienstliche Mitteilung handelt. Der Versand und Empfang einer privaten E-Mail am Arbeitsplatz wird durch das **Fernmeldegeheimnis** in Art. 10 Grundgesetz (GG) und § 85 Abs. 1 Telekommunikationsgesetz (TKG) geschützt. Dieses umfasst sowohl den Kommunikationsinhalt als auch 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 überwachen. Dagegen unterliegen dienstliche E-Mails der Schulleitung gegenüber nicht dem Fernmeldegeheimnis.

Wird auch den Schüler/innen der private E-Mail-Verkehr gestattet, entsteht möglicherweise ein Spannungsverhältnis zwischen dem Erziehungsauftrag der Schule auf der einen und dem Anspruch auf Datenschutz und Wahrung des Fernmeldegeheimnisses der Schüler/innen auf der anderen Seite. Auch die freie E-Mail-Kommunikation der Schüler/innen außerhalb des Unterrichts in der Schule unterliegt nämlich dem Fernmeldegeheimnis und ist deshalb einer Kontrolle entzogen. Eine Kontrollbefugnis der Schule lässt sich nicht aus der aus ihrem Erziehungsauftrag resultierenden Aufsichtspflicht herleiten, da diese Pflicht nur so weit reichen kann, wie Lehrkräfte Kenntnis von E-Mail-Nachrichten nehmen dürfen. Wegen des Fernmeldegeheimnisses sind sie dazu aber 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 möglicherweise strafrechtlich relevanten Kommunikation, bleibt – neben der schulinternen Maßnahme eines (vorläufigen) Ausschlusses von der Nutzung – nur der Weg, Strafanzeige zu erstatten, um den Tatbestand aufzuklären.

Wenn die Schule den privaten Gebrauch des Internets außerhalb des Unterrichts ermöglicht, vermittelt sie im Übrigen je nach Art des Angebots den Zugang zur Nutzung entweder von **Medien- oder Telediensten**. Sie ist insoweit **Diensteanbieterin** im Sinne des § 3 Nr. 1 Teledienstegesetz (TDG) und des § 2 Nr. 1 Teledienstedatenschutzgesetz (TDDSG) bzw. des § 3 Nr. 1 Mediendienste-Staatsvertrag (MDStV). Deshalb hat sie der besonderen aus diesem Anbieterstatus erwachsenden medienrechtlichen Pflichtenstellung Rechnung zu tragen. Dazu gehören insbesondere die Wahrung der Unterrichtspflichten nach §§ 3 Abs. 5 TDDSG, 12 Abs. 6 MDStV und die datenschutzrechtlichen Pflichten nach Maßgabe der §§ 4 TDDSG, 13 MDStV. Sie muss außerdem allen berechtigten Nutzer/innen auf deren Wunsch Auskunft gemäß §§ 7 TDDSG, 16 MDStV erteilen.

Fraglich ist, ob und inwieweit die Schule darüber hinaus für das Nutzungsverhalten ihrer Schüler/innen im WWW 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 kommunikationsrechtlich nicht für die fremden Inhalte verantwortlich ist, wird jede Schule aus schul- und jugendschutzrechtlichen Gründen 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.

Wegen der Einzelheiten wird insgesamt auf die gesetzlichen Regelungen im TKG, TDG, TDDSG und dem MDStV verwiesen (vgl. im Übrigen auch Kapitel 5.2.). Eine vertiefende Darstellung findet sich bei Johann Bizer „Schüler am Netz: Rechtsfragen beim Einsatz von E-Mail, Newsgroups und WWW in Schulen“, in: Lernort Multimedia, Jahrbuch Telekommunikation und Gesellschaft Band 6, 1998, S. 244 ff..

## **4.2 Zugangskontrollen**

Einige Schulen legen in Computerräumen und Medienecken Listen aus, in die sich die Benutzer/innen der PCs mit Namen und weiteren 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 nach § 19 Abs. 1 Satz 1 SchVG 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 innerhalb des Betriebssystems oder der Einsatz einer zusätzlichen Sicherheitssoftware, mit der automatisch jede PC-Nutzung protokolliert wird. Das Protokoll sollte nur von der Administration gelesen werden können. Der Zugang zum System ist dann auch nur über einen Benutzernamen und die Eingabe eines individuellen Passwortes möglich. Selbstverständlich muss das Passwort so ausgestaltet sein, dass es nicht ohne Weiteres ausgeforscht und von anderen verwandt werden kann. Die bei der Protokollierung entstandenen Verbindungsdaten dürfen im Übrigen nicht zu Kontrollen der Netzaktivitäten der Nutzer/innen genutzt werden und sind unverzüglich zu löschen.

## **5. 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. -bezieharen 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.

## 5.1 Inhaltsdaten: Was darf ins Internet?

### 5.1.1 Grundsätzliches

Soweit die Bereitstellung von Daten im Internet ohne Einschränkungen erfolgt, also keine geschlossene 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 speziellen datenschutzrechtlichen Bestimmungen des Schulrechts sowie ergänzend dazu nach den allgemeinen Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW).

Nach Maßgabe des § 4 Abs. 1 DSG NRW ist die Verarbeitung personenbezogener Daten nur zulässig, wenn

- a) eine Rechtsvorschrift sie erlaubt 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 betroffene Person auf die Einwilligung schriftlich besonders hinzuweisen. Sie ist in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, bei einer beabsichtigten Übermittlung über die Empfänger/innen der Daten aufzuklären; sie ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass sie die Einwilligung verweigern und mit Wirkung für die Zukunft widerrufen kann. Die Einwilligung kann auch elektronisch erklärt werden, wenn sichergestellt ist, dass

1. sie nur durch eine eindeutige und bewusste Handlung der handelnden Person erfolgen kann,
2. sie nicht unerkennbar verändert werden kann,
3. ihre Urheberin oder ihr Urheber erkannt werden kann,

4. die Einwilligung bei der verarbeitenden Stelle protokolliert wird und
5. der betroffenen Person jederzeit Auskunft über den Inhalt ihrer Einwilligung gegeben werden kann.

### Einwilligung

Voraussetzungen einer wirksamen Einwilligung sind also:

- **Informiertheit**  
Die Betroffenen müssen umfassend über die Verarbeitung unterrichtet werden. Sie müssen dabei auch über die Risiken einer solchen weltweiten Veröffentlichung aufgeklärt werden. Außerdem sind sie darauf hinzuweisen, dass ihnen aus der Verweigerung einer Einwilligung keine Nachteile entstehen.
- **Freiwilligkeit**  
Eine wirksame Einwilligung liegt nur vor, wenn sie freiwillig erteilt worden ist. Das setzt insbesondere auch voraus, dass die Entscheidung frei von (sozialem) Druck getroffen wurde. Freiwillig ist eine Einwilligung ferner auch nur dann, wenn überhaupt eine Handlungsalternative besteht.
- **Widerrufbarkeit**  
Die Betroffenen sind darauf hinzuweisen, dass sie die Einwilligung jederzeit widerrufen können, wo und bei wem der Widerruf zu erklären ist und welche Folgen er hat (dass nämlich alle personenbezogenen/-bezieharen Daten unverzüglich zu löschen sind).
- **Form**
  - Die Einwilligung bedarf grundsätzlich der **Schriftform**.
  - **Ausnahme:** Wegen besonderer Umstände ist eine andere Form angemessen.
  - Sie kann ausnahmsweise elektronisch erklärt werden, wenn die besonderen Voraussetzungen hierzu erfüllt sind.

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.

Was bedeutet dies alles nun konkret in der und für die Schulpraxis? Im Folgenden werden verschiedene Fallgruppen mit ihren spezifischen Problemen behandelt.

#### **5.1.2 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 ins Netz eingestellt wird, ohne dass die Betroffenen hiervon vorher unterrichtet wurden. 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 allein § 19 a Abs. 1 Satz 1 Schulverwaltungsgesetz (SchVG) in Verbindung mit § 29 Abs. 1 Satz 2 DSGVO NRW in Betracht. Danach könnte eine Veröffentlichung personenbezogener Daten von Lehrer/innen im Internet auf dieser Rechtsgrundlage nur erfolgen, wenn sie zur Aufrechterhaltung des Dienstbetriebes erforderlich wäre, soweit hier also die Kommunikation der Schule mit der Öffentlichkeit zum Schulbetrieb gehören würde. Aber auch dann wären Lehrkräfte über die geplante Veröffentlichung vorher zu informieren. Bei Einwendungen – wegen persönlicher Bedenken – muss die Schulleitung im Einzelfall die Interessen der Schule gegen die schutzwürdigen Interessen der betroffenen Lehrkraft abwägen. Im Hinblick auf die enge lokale Begrenzung des Aufgaben- und Wirkungsbereichs von Schulen dürfte in aller Regel das Persönlichkeitsrecht der betroffenen Lehrkraft Vorrang vor dem Informationsinteresse einer breiten Öffentlichkeit (Internetnutzer/innen) haben.

Da die Notwendigkeit der Veröffentlichung von Daten nicht immer zweifelsfrei festgestellt werden kann und gerade im Bereich der Schule ohnehin die Ausnahme bildet, sollte – auch im Sinne einer möglichst hohen Akzeptanz im Kollegium – grundsätzlich vor jeder Einstellung personenbezogener Daten ins Internet die ausdrückliche Einwilligung der betroffenen Lehrer/innen zu dieser Veröffentlichung eingeholt werden. Einer (zusätzlichen) Einwilligung bedarf es im Übrigen immer auch dann, wenn das **Foto** einer Lehrkraft auf der Homepage veröffentlicht werden soll, und zwar unabhängig davon, ob eine Namensangabe hinzugefügt ist oder nicht. Sie ist hier allein bereits wegen des Rechts am eigenen Bild erforderlich.

Datenschutzrechtlich nicht unproblematisch ist die Veröffentlichung eines täglich wechselnden **Vertretungsplans** auf der Homepage, wie sie an mehreren Schulen geplant war. Eine weltweite Veröffentlichung ist auf jeden Fall unzulässig, da sie nicht zur Aufgabenerfüllung der Schule erforderlich ist. In Betracht kommt allenfalls, einer geschlossenen Benutzergruppe den Zugriff auf einen solchen Plan zu ermöglichen. Fraglich ist dabei, welche Personen (alle Lehrkräfte der Schule oder auch alle Schüler/innen und Erziehungsberechtigten) vom privaten PC aus den digitalen Vertretungsplan lesen können sollen. Zur Aufgabenerfüllung ist es nicht erforderlich, dass Personen (Kolleg/inn/en, Schüler/innen, Eltern), für die der Unterrichtsausfall keine Konsequenzen hat, darüber Kenntnis erlangen, welche Lehrkraft in welcher Unterrichtsstunde vertreten wird. Ob sichergestellt werden kann, dass auch Dritte aus den Angaben im Vertretungsplan kein Verhaltensprofil über eine Lehrkraft erstellen (also etwa über krankheitsbedingte Fehlzeiten oder regelmäßige, funktionsbedingte Abwesenheiten usw. der vertretenen Person), erscheint zweifelhaft. Jedenfalls ist davon auszugehen, dass alle Angaben im Plan – auch ohne Angabe des Namens – mit dem Zusatzwissen der Zugriffsberechtigten (in der Schulöffentlichkeit) immer personenbezogen sein werden. Selbst wenn es gelingt, nur berechtigten Personen die jeweils für sie in Frage kommenden Angaben zugänglich zu machen, bleibt ein „Restrisiko“ der missbräuchlichen Datennutzung. Auch in diesem Fall müssen alle Beteiligten über die Verfahrensweise unterrichtet werden und ihre Einwilligung erteilen. Damit dürfte das Vorhaben eines digitalen Vertretungsplanes nur schwer zu verwirklichen sein. Sobald eine Lehrkraft nicht mitmacht, lässt es sich nicht mehr umsetzen. Eine Alternative könnte eventuell ein gut organisiertes Benachrichtigungssystem mittels verschlüsselter E-Mail sein.

### 5.1.3 Daten von Schüler/innen und Erziehungsberechtigten

Personenbezogene Daten von Schüler/innen (zum Beispiel Klassensprecher/innen, Gewinner/innen eines Wettbewerbs, Schulrekordhalter/innen) und von Erziehungsberechtigten (zum Beispiel Vertreter/innen eines Schulmitwirkungsorgans) dürfen nach § 19 Abs. 2 SchVG in Verbindung mit § 4 DSG NRW grundsätzlich nur mit Einwilligung auf der Homepage veröffentlicht werden. Ob die Daten einer oder eines Jugendlichen ins Internet eingestellt werden dürfen, entscheidet allerdings mit ihrer oder seiner wachsenden Reife immer seltener die erziehungsberechtigte Person. Vielmehr bestimmt § 19 Abs. 2 Satz 3 SchVG, dass minderjährige Schüler/innen in Bezug auf die Erhebung und Verarbeitung ihrer Daten selbst **einwilligungsfähig** sind, 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, aber auch Jugendliche, die die Klassen 9. und 10 besuchen, dürften überwiegend über die erforderliche Einsichtsfähigkeit verfügen. Letztlich lässt sich die Einsichtsfähigkeit allerdings nur einzel-fallbezogen beurteilen.

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 Erziehungsberechtigten wirksam einwilligen; ist die Vertrauenslehrerin, der Klassenlehrer oder eine andere Person mitfotografiert worden, muss ebenfalls die Einwilligung eingeholt werden. Fehlt es an einer der erforderlichen Einwilligungen oder ist eine dieser Erklärungen unwirksam (zum Beispiel weil sie nicht freiwillig, sondern nur auf Gruppendruck abgegeben wurde), 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.

### 5.1.4 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 zur Zeit 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. 5.1.1) ist die Aufnahme personenbezogener Daten in eine solche elektronische Liste unzulässig.

### 5.1.5 Beiträge von Schüler/innen

Da, wie eingangs ausgeführt, 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 5.1.4 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. Hier gelten die Regelungen des § 25 SchVG und des § 37 Allgemeine Schulordnung (ASchO). Nicht die Schule, sondern die Redaktion der Schülerzeitung trägt die Verantwortung für den 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.

### 5.1.6 Webcams

Es gibt erste Anfragen, ob auf dem Schulgelände Kameras (sogenannte Webcams) installiert und deren Bilder im Internet abrufbar gespeichert werden dürfen. Dies begegnet dann keinen datenschutzrechtlichen Bedenken, wenn die Kameras so aufgestellt sind, dass die anfallenden Bilder keine Daten mit Personenbezug enthalten. Ein Personenbezug ist auf jeden Fall herstellbar, wenn Gesichter oder andere identifizierende Merkmale erkennbar sind oder durch Aufnahmesteuerung oder Bildbearbeitung seitens der Empfängerin oder des Empfängers erkennbar gemacht werden können. In Frage kommen daher allenfalls **Übersichtsaufnahmen**, die die Herstellung eines Personenbezugs 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 (z.B. anhand von Fotos, auf denen leere Räume abgebildet sind) übermittelt werden können.

Eine Übertragung personenbezogener Bilder ins Internet ist nur dann zulässig, wenn zuvor alle betroffenen Personen bzw. ihre Erziehungsberechtigten wirksam in die Veröffentlichung per Internet eingewilligt haben (vgl. 5.1.1).

## 5.2 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 mithin 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.

Welchen Informationspflichten muss nun eine Schule als Anbieterin Rechnung tragen?

### 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 und 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.

### **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 Weitervermittlung ermöglicht. Auch sollte jederzeit erkennbar sein, wer für die aufgerufene Seite verantwortlich ist. Es kann irreführend sein, wenn zum Beispiel der 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.

### **Informationspflichten**

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.

**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 für 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.

**Transparenz durch Datenschutzpolicies**

Wer es mit dem Selbstbestimmungsrecht der Nutzer/innen ernst meint, sollte darüber hinaus Datenschutzhinweise, auch bekannt als Datenschutzpolicies, auf der Homepage platzieren. Damit wird offengelegt, wie mit automatisch anfallenden Daten – den Spuren im Netz – umgegangen wird und ob überhaupt 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 per-

sonenbeziehbar 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.

**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.

## 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. Für die Entscheidung über den Erlass einer solchen Ordnung ist nach § 5 Abs. 2 Nr. 15 Schulmitwirkungsgesetz die Schulkonferenz zuständig. Dadurch wird sichergestellt, dass sowohl Vertreter/innen der Lehrer/innen als auch der Erziehungsberechtigten und – sofern es sich nicht um eine Schule der Primarstufe handelt – auch der Schüler/innen an der Entscheidung über den Interneteinsatz und dessen Kontrolle an ihrer Schule beteiligt werden. Eine solche Mitbestimmung erhöht erfahrungsgemäß die Akzeptanz der getroffenen Regelungen, dürfte aber zudem auch dazu beitragen, die Bestimmungen für alle beteiligten Personengruppen transparenter zu gestalten.

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 alle nordrhein-westfälischen 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. Das macht eine allgemeingültige Aussage zu einer "Muster"-Benutzungsordnung schwierig. Trotzdem sollen an dieser Stelle einige grundsätzliche Überlegungen dargestellt werden, welche Festlegungen in einer Nutzungsordnung getroffen bzw. nicht getroffen werden können.

### **In einer Nutzungsordnung wird insbesondere Folgendes zu regeln sein:**

- 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.