Der Landesbeauftragte für Datenschutz
Saarland

Saarbrücken, den 20.06.2003
Tel.: 0681/94781-36

Merkblatt
„Schulen ans Netz - mit Sicherheit“

Im Zuge der Programme „Schulen ans Netz“ und „Lehren für die Zukunft“ nutzen immer mehr saarländische Schulen die faszinierenden technischen Möglichkeiten des Internet. Dabei ergeben sich neben vielen handwerklichen Problemen auch Fragen zum sicheren, datenschutzgerechten Umgang damit. Dieses Merkblatt soll Schulleitungen, Lehrerinnen und Lehrern, Schülerinnen und Schülern sowie Eltern kurz gefasste Hinweise und Empfehlungen aus Sicht des Datenschutzes geben. Es soll die nötige Sensibilität für Sicherheits- und Datenschutzprobleme vermittelt und praktische Lösungen für weitere Fragestellungen vorgestellt werden, um mit den Herausforderungen des Internet konstruktiv und sachgerecht umzugehen. Dieses Merkblatt und weitere Materialien zum Internet können auch aus dem Internet-Angebot des Landesbeauftragten für Datenschutz (LfD) unter: www.lfd.saarland.de abgerufen werden.

Was hat das Internet mit personenbezogenen Daten zu tun?

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, Berufsbezeichnung, Zeugnisnoten, Klassenzugehörigkeit, Funktion in der Schule. 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. Zu den personenbezogenen Daten gehören aber auch Bilder, Filme, Sprachaufzeichnungen, eMails, Foren-/Gästebücher-/Chat-Beiträge sowie die Bestands-, Verbindungs- und Abrechnungsdaten bei Service-Providern.

Internet-Angebote der Schulen enthalten in der Regel personenbezogene Daten der Lehrer, Schüler und evtl. sogar der Eltern. In Deutschland ist eine Verarbeitung (dazu gehört auch die Aufnahme in Internet-Angebote und die Präsentation) von personenbezogenen Daten nur zulässig, wenn entweder ein Gesetz dies erlaubt oder der Betroffene in diese Verarbeitung schriftlich eingewilligt hat. Zum Schutz personenbezogener Daten ist in § 4 des

Saarländischen Datenschutzgesetzes SDSG als Ziel vorgegeben, so wenig personenbezogene Daten wie möglich zu verarbeiten. Die Datenschutzbestimmungen des **Saarländischen Schulordungsgesetzes (§ 20 b SchoG**) erlauben eine Verarbeitung von Schüler- und Elterndaten nur, wenn dies zur Erfüllung des Unterrichts- und Erziehungsauftrages der Schule erforderlich ist. Im strengen Sinne erforderlich ist eine Internet-Präsentation der Schule nicht, so dass nur eine **Zustimmung** zur Verarbeitung gemäß § 4 des **SDSG** als rechtliche Grundlage in Frage kommt. Diese Einwilligung ist nicht nur eine formale, sondern setzt bei dem Betroffenen ausreichende Informationen über die geplante Nutzung und die damit verbundenen Risiken voraus. Die Einwilligung muss völlig freiwillig erfolgen und kann jederzeit widerrufen werden, wonach alle widerrufenen Daten zu löschen sind. Bei Minderjährigen ist die Einwilligung von den Erziehungsberechtigten einzuholen. Ein Muster für eine solche Einwilligungserklärung ist unserem Internet-Angebot im Abschnitt „Internet“ unter www.lfd.saarland.de zu entnehmen.

Unter **Datenverarbeitung** ist jeder Umgang mit personenbezogenen Daten zu fassen, das heißt im Einzelnen das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie das sonstige 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.

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 IP-Adressen und eMail-Adressen benutzt und **Datenspuren** auf dem eigenen Rechner, den Netzknoten und bei den Service-Providern 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. eMail-Adressen in Internet-Angeboten werden in der Regel für Werbezwecke ausgewertet und weiterverkauft.

Suchmaschinen durchsuchen im Laufe der Zeit alle verfügbaren Internet-Angebote bzw. Gästebücher, Newsgruppen und Foren und werten diese nach brauchbaren Stichworten aus;

dazu gehören z. B. auch Namen und eMail-Adressen. Die Stichworte und die zugehörigen Fundstellen werden in umfangreichen Datenbanken gespeichert und können von Jedermann durch Aufruf einer Suchmaschine und Eingabe beliebiger Stichworte ausgewertet werden. Insbesondere können dann durch Eingabe eines Namens sofort alle Internet-Angebote und alle Forenbeiträge des Betroffenen aufgefunden, zusammengefasst und daraus z. B. ein Persönlichkeitsprofil erstellt werden. Firmen haben sich inzwischen darauf spezialisiert, solche Profile gegen Geld z. B. bei Einstellungen von Personal, neuen Geschäftsverbindungen oder Nachforschungen anzubieten. Wegen der oft ausländischen Betreiber ist ein gesetzlicher Berichtigungs- oder Löschungsanspruch nicht durchsetzbar. Einträge in Suchmaschinen bleiben auch dann (unter Umständen lebenslang) bestehen, wenn das zu Stichworten gehörige Angebot geändert oder gelöscht worden ist. Homepages von Schulen oder elektronische Visitenkarten von Schülern oder Lehrern tragen zur Profilbildung entscheidend bei.

Der Schutz personenbezogener Daten ist inzwischen auch bedroht durch die zunehmenden Archivierung von Internet-Seiten und Newsgruppen-Beiträgen. So speichert das Projekt Wayback-Machine unter www.archive.org seit 1996 die alle 2 Monate weltweit abgezogenen Internet-Seiten, so dass es möglich ist, mit Angabe der URL entsprechende frühere Angebote wieder herzustellen und auch in der historischen Entwicklung zu betrachten. Eine Stichwortsuche in dem Archiv, das Anfang 2003 ca. 10 Mia. Dokumente in einem Datenumfang von ca. 100 Terabyte auf ca. 200 Rechnern enthielt, ist derzeit noch nicht möglich. Das Usenet-Archiv, in dem die Newsgroup-Einträge archiviert werden, rühmt sich, solche Einträge bis zurück in das Jahr 1981 zu besitzen und u. A. alte Postings bekannter Personen finden zu lassen, wie z. B. Tim Barners-Lee, der das WWW erfunden hat oder Linus Thorwalds, der Linux entwickelt hat. Auch das beliebte Auktionsportal Ebay speichert seit 1995 alle Auktionen und stellt diese Daten z. B. für Zugriffe der Nachrichtendienste oder Strafverfolgungsbehörden zur Verfügung. Auch hier gilt, dass wegen der oft ausländischen Betreiber ein gesetzlicher Berichtigungs- oder Löschungsanspruch nicht durchsetzbar ist, so dass die Daten (und in Beiträgen enthaltene Denk- bzw. Verhaltensweisen) eines Betroffenen unter Umständen ein Leben lang „an ihm haften“ bleiben, was (vor allem bei jungen Menschen) unter Umständen zu von ihm nicht gewollten Folgen führen kann.

Aktive Inhalte (z. B. Java-Scripts, ActiveX-Controls) und Cookies können missbraucht werden, um Benutzerdaten und das Benutzerverhalten auszuspionieren, kritische Daten vom Rechner des Benutzers ins Internet abzuziehen oder das Betriebsystem oder Dateien zu manipulieren oder gar zu löschen.

Über das Internet oder eMail bezogene Programme können Viren enthalten, die kritische Daten über das Internet versenden oder den eigenen Rechner schädigen.

Auf Computern gespeicherte Passwort-Dateien können mit Hilfe von im Internet verfügbaren Crack-Programmen entschlüsselt oder über das Internet laufende Passworte mitgelesen und missbräuchlich verwendet werden.

Von verschiedenen Computer-Zeitschriften werden einfach zu nutzende CD´s mit einem bootbaren Linux-Betriebssystem angeboten (z. B. Knoppix-CD), die zusätzlich zu der erwünschten Nutzungsmöglichkeit eines alternativen Betriebssystems auch Programme enthalten, die Dateien anderer Betriebssysteme unter Umgehung der dortigen Schutzeinrichtungen unerkannt manipulieren oder Lesen können oder den Datenverkehr von Inhouse- oder Funknetzen mitlesen lassen, so dass auch z. B. Zugangsberechtigungen aufgedeckt und von Unbefugten missbräuchlich verwendet werden können.

Über USB-Schnittstellen können inzwischen auch externe Speicher wie z. B. USB-Stifte („Memory-Sticks“) oder PDA´s angeschlossen werden, mit denen ein einfacher, umfangreicher Datentransfer möglich ist oder über die sogar ein fremdes Betriebssystem mit freier Zugriffsmöglichkeit auf den vorhandenen Rechner bootbar ist.

Kostenlose oder durch Werbung finanzierte kostengünstige Angebote z. B. für Web-Hosting, Foren, Gästebücher, eMail-Service, Super-Software, Videoplayer sollten wegen der damit verbundenen Risiken vermieden werden. Oft werden Daten und Adressen der Zugreifer (auch unerkannt) gesammelt und weiterverkauft bzw. zu Werbezwecken verwendet.

Wie kann man sich selbst schützen?

Zum Selbstdatenschutz gehören alle Maßnahmen, die darauf abzielen, eine vom Nutzer nicht gewollte Verarbeitung seiner personenbezogenen Daten zu verhindern, z. B. Sicherheitseinstellungen, Inhaltsschutz durch Verschlüsselung, Anonymität und Pseudonymität, Transparenz und Selbstbestimmung bei jeder Kommunikation.

Ganz wichtig dabei ist eine sichere Einstellung des Betriebssystems (z. B. Anzeige aller Dateien mit allen Dateierweiterungen im Explorer des Betriebssystems, Deaktivierung von VBS) und eine sichere Konfiguration der Browser (neueste Browser-Version und Updates, Sicherheitseinstellungen zur Erkennung/Ablehnung von Cookies oder aktiven Inhalten, Vermeiden von Plug-Ins). Es gibt auch seriöse Angebote, bei denen man den eigenen Internet-PC auf Sicherheitsmängel untersuchen lassen kann wie z. B. durch einen Browser-Test unter

www.lfd.niedersachsen.de. Ganz wichtig ist auch, dass man bei der Gestaltung von Internet-Angeboten einen Personenbezug so weit es geht vermeidet, bei Foren und Chats möglichst mit Pseudonymen („Nickname“) bzw. anonym teilnimmt.

Der eigene PC sollte gegen missbräuchlichen Zugriff abgesichert sein. Das Bios sollte so eingestellt sein, dass ein Booten nur von der Systemplatte möglich ist. Das Betriebssystem sollte die Aktivierung neuer Laufwerke über USB-Speicher verhindern. Passworte oder Pins sollten grundsätzlich nicht gespeichert werden; dies gilt vor allem dann, wenn mehrere Personen Zugriff haben.

Weiterhin ist ein leistungsfähiger Virenscanner unverzichtbar und zusätzlich kann der PC bzw. das Netz bei der Internet-Nutzung noch durch eine Firewall abgesichert werden, die verhindert, dass Unbefugte auf den Rechner zugreifen oder unerkannt Daten übermittelt werden. Nebenbei sollte man manuell oder automatisch die eigenen Datenspuren auf dem PC löschen (besuchte Adressen und Seiten, Cookies). Sollte ein Angebot ohne Cookie-Nutzung oder Freigabe aktiver Inhalte nicht zu nutzen sein, sollte man aus Sicherheitsgründen darauf verzichten.

Außerdem kann man sich vor missbräuchlicher Verwendung seiner Daten schützen, in dem man sich so wenig wie möglich in Internet-Angebote aufnehmen lässt und vor allem auch eigene Webseiten („elektronische Visitenkarten“) vermeidet. Die Präsentation von Daten von Verwandten, Freunden und Bekannten auf den eigenen Seiten setzt zudem ebenfalls eine Einwilligung der Betroffenen dazu voraus.

Bei kostenlosen Newslettern oder sonstigen Informationsbriefen sollte man so wenig wie möglich eigene Daten weitergeben; in der Regel sollte hier die eMail-Adresse ausreichend sein. Bei allen Formularen sollte man immer prüfen, welche Daten erforderlich sind und nicht automatisch alle Felder ausfüllen. Sinnvoll ist es, in Newsgruppen, Foren und Chats möglichst anonym oder mit leicht löschbaren Mail-Adressen zu operieren, um eine gefährliche Identifikation oder Mail-Bomben zu vermeiden.

Der Austausch von Dokumenten in Formaten, die Makros unterstützen oder unsichtbar personenbezogene Informationen beifügen, sollte vermieden werden. Statt dessen können Formate wie RTF oder HTML verwendet werden. Falls empfangene Word-Dokumente nur betrachtet werden sollen, können die Programme "Wordview" oder „Wordpad“ (in Windows enthalten) verwendet werden, die die Ausführung von Makros nicht unterstützen. Kritische eMails und ihre Anlagen sollten verschlüsselt werden.

Wer trägt die Verantwortung für den Internetzugang und das Internet-Angebot der Schule und wo ist geregelt, was erlaubt ist?

Grundsätzlich trägt die Schulleitung, die den Zugang zum Internet eröffnet, die Verantwortung für den Internetzugang der Schule. Jede Schule sollte verbindliche Regeln festlegen:

- 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.

Entsprechende Entwürfe enthält das Internet-Angebot des LfD unter www.lfd.saarland.de.

Was muss man bei einer schuleigenen Homepage beachten?

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.

Bei den Internet-Angeboten **sollte ein Personenbezug wegen der damit verbundenen Risiken für die Bildung von Persönlichkeitsprofilen und der fast unbegrenzten Speicherungsmöglichkeiten vermieden werden**. Gegebenenfalls wäre eine Nennung von Vornamen hinnehmbar. Vor der Aufnahme von personenbezogenen Daten sollte von dem Betroffenen (Lehrer, Schüler, Eltern, Projektpartner) die **Einwilligung** unter den zu Anfang bei „Datenschutz“ genannten Voraussetzungen eingeholt werden (Muster einer Einwilligung unter www.lfd.saarland.de). Ist der Betroffene nicht volljährig, ist die Einwilligung des Erziehungsberechtigten unter den gleichen Voraussetzungen erforderlich.

Zur Konzeption des Angebotes ist der interne **Datenschutzbeauftragte der Schule hinzuzuziehen**, um sicherzustellen, dass die datenschutzrechtlichen Anforderungen beachtet werden. Er führt auch eine Vorabkontrolle nach § 11 SDSG durch. Vor der Freigabe, d. h. der öffentlichen Nutzbarkeit, ist **nach § 7 SDSG der Landesbeauftragte für Datenschutz zu beteiligen**.

Bei **Links** sollte klar herausgestellt werden, dass damit der Bereich der Schule verlassen wird und diese die Verantwortung für die dann folgenden Inhalte nicht übernimmt. Das Angebot sollte so gestaltet sein, dass dann auch eventuelle Schulrahmen gelöscht werden, um nicht den Eindruck zu erwecken, dass das gelinkte Angebot ein Teil des Schulangebots ist (siehe auch Datenschutzinfo unter www.saarland.de).

Bei **eMail-Adressen** oder Mitteilungsformularen sollte auf die Risiken des offenen Versands und auf die Alternative des Briefpost- oder Fax-Versandes hingewiesen werden (siehe Datenschutzinfo unter www.saarland.de). Nützlich wäre auch das Angebot eines verschlüsselten eMail-Austausches oder eine SSL-geschützte, verschlüsselte Übertragung von Formularen.

Die Eingangsseite muss eine **Anbieterkennzeichnung/Impressum** mit Name und Anschrift enthalten, die von jeder Webseite aus erreichbar sein sollte. Zusätzlich sollten gleich zu Anfang über eine **Datenschutz-Policy** die Rahmenbedingungen, unter denen das Angebot genutzt werden kann, deutlich gemacht werden. Dazu gehört auch, dass keine Gewähr für die Richtigkeit der angebotenen Informationen übernommen werden kann und eine Haftung für Einträge Dritter oder Rechtsverletzungen auf gelinkten Seiten abgelehnt wird (siehe auch Datenschutzinfo unter www.saarland.de).

Gästebücher, Foren und Chats müssen regelmäßig auf strafrechtlich relevante Meinungsäußerungen und datenschutzrechtlich unzulässige Einträge hin überprüft und diese entfernt werden. Auf die damit verbundenen Risiken sollte in der Datenschutzpolicy und vor jedem Eintrag hingewiesen werden (siehe Datenschutzinfo unter www.saarland.de).

Bei der Auswahl von **Service-Providern** sollte darauf geachtet werden, dass sie dem EU-Recht unterliegen und in den AGB deutlich klargestellt wird, dass diese erkannt haben, dass für sie das TDG und das TDDSG gilt und dass die im Rahmen des Vertragsverhältnisses anfallenden Daten (Bestands-, Verbindungs- und Abrechnungsdaten) nur zur Abwicklung der Dienstleistung verwandt werden, gelöscht werden, wenn sie nicht mehr erforderlich sind, und nicht an Dritte weitergeben werden.

Kostenlose Angebote von Web-, eMail-, Foren- und Gästebücher-Services, die in der Regel durch Werbung oder Auswertungen des Nutzerverhaltens finanziert werden, sollten vermieden werden. Bei der Nutzung solcher kostenloser Angebote sollte darauf geachtet werden, dass die eben bei Service-Providern dargestellten Bedingungen ebenfalls erfüllt sind

und dass bei der Nutzung keine unerkannten Nebeneffekte (z. B. automatische Weiterleitung von Zugreiferdaten) auftreten können.

Aktive Inhalte und **Cookies** sollten wegen eventueller Sicherheitsrisiken grundsätzlich vermieden werden. Sollten aktive Inhalte zur Attraktivitätssteigerung des Angebots unbedingt genutzt werden, muss das Angebot so gestaltet sein, dass es auch ohne deren Aktivierung nutzbar bleibt. Das Angebot der Schule darf nicht dazu führen, dass der Zugreifer seine Sicherheitseinstellungen aufgeben muss, um es vollständig nutzen zu können.

Für die **Veröffentlichung eigenständiger Beiträge von Schülern** ist eine vorherige Genehmigung des Verantwortlichen erforderlich, da die Schulleitung oder die von ihr beauftragte Lehrkraft für die Homepage letztlich verantwortlich ist. Eine Ausnahme stellt die Veröffentlichung der Schülerzeitung auf der Homepage dar. Da Redaktion und Herausgeber der Schülerzeitung die Verantwortung für deren Inhalt tragen (§ 13 Allgemeine Schulordnung), ist es zur Verdeutlichung dieser Verantwortung sinnvoll, die Schülerzeitung auf einer eigenen Homepage mit eigenem Domainnamen auf dem Schulserver zu veröffentlichen.

Klassenlisten, Ehemaligenlisten, Arbeitsgruppenbeschreibungen, Projektteilnehmer, Elternvertretungen oder Sprechstundenübersichten im Internet-Angebot dürfen nur ins Internet-Angebot übernommen werden, wenn die Einwilligung der Betroffenen dazu vorliegt (Muster-Einwilligung unter www.lfd.saarland.de). Solche Veröffentlichungen sollten wegen der damit verbundenen Risiken möglichst vermieden werden.

Auch **Bilder** sind personenbezogene Daten, wenn darauf Personen zu erkennen sind. Wie bei allen personenbezogenen Daten gilt auch hier die Anforderung der Einwilligung unter den oben genannten Bedingungen in jedem Einzelfall. Gegen unbefugte Verbreitung ist das Recht am eigenen Bild durch das Kunsturhebergesetz besonders geschützt. Nach der Rechtsprechung sind Bildveröffentlichungen ohne Einwilligung nur unter bestimmten Voraussetzungen bei sog. „Personen der Zeitgeschichte“ und ansonsten nur unter bestimmten, von der Rechtsprechung entwickelten, zum Teil engen Voraussetzungen zulässig.

Dies gilt auch für **Webcam-Aufnahmen.** Sie dürfen generell nur ins Internet gestellt werden, wenn die Kameras so aufgestellt sind, dass die Bilder keine Daten mit Personenbezug enthalten, also in der Regel bei bloßen Übersichtsaufnahmen, die keine Identifizierung erlauben.

Als **Muster** für ein aus Sicht des Datenschutzes unkritisches Internet-Angebot einer (kleinen) Schule verweise ich auf http://home.t-online.de/home/gs-wellesweiler.

Ist eine private Nutzung des Internet-PC der Schule erlaubt und was ist dabei zu beachten?

Private Nutzung ist dann gegeben, wenn dabei Internet-Zugriffe oder eMail-Transfers erfolgen, die ohne Bezug zur Schule bzw. zum Unterricht stehen. Insofern ist die Beschaffung von Informationen durch Schüler oder Lehrer zur Unterrichtsvorbereitung keine private Nutzung.

Wird eine **private Nutzung** zugelassen, handelt die Schule auch den eigenen Lehrkräften und Schülern gegenüber als Teledienstеanbieter und unterfällt damit den Pflichten nach dem Teledienstgesetz (TDG) und dem Teledienstedatenschutzgesetz (TDDSG). 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 eMail-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 (z. B. getrennte Server) nicht möglich, so ist die gesamte Kommunikation wie die private Nutzung zu behandeln; sie unterfällt damit insgesamt dem Fernmeldegeheimnis. Damit dürfte dann auch die Nutzung im Rahmen des Unterrichts oder Dienstbetriebs nicht mehr überwacht werden.

Ist eine Kontrolle der Internet-/eMail-Nutzung erlaubt bzw. wie kann man das Abrufen kritischer Seiten verhindern?

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 gem. § 84 des Saarländischen Personalvertretungsgesetzes (SPersVG). 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 Benutzerordnung der Schule. Lehrerinnen und Lehrer können im Unterricht Einsicht in die Netzaktivitäten ihrer Schülerinnen und Schüler nehmen, denn der Unterricht liegt in der Verantwortung der Lehrkraft. Lehrkräfte haben selbstverständlich keine generelle Einsichtsberechtigung in die Protokolle aller Netzaktivitäten der Schule.

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.

Kann ich Internet-Server, Internet-Zugänge oder sonstige Unterrichtsprogramme auf dem gleichen Rechner/Netz betreiben, auf dem Schulverwaltungsdaten bearbeitet werden?

Nein. Aus Sicherheitsgründen muss durch eine physikalische Abschottung der Rechner und der Netze ein Schutz der Schulverwaltungsdaten gewährleistet werden. Das Ministerium für Bildung, Kultur und Wissenschaft hat dies auch in einer Verordnung so geregelt.

Wo finde ich ausführliche Informationen und Tips zum Computer-Einsatz und zur Internet-Nutzung?

Umfangreiche und sehr detaillierte Angaben von Risiken, technischen Informationen und geeigneten Maßnahmen zur Datensicherheit bietet das **IT-Grundschutzhandbuch** des Bundesamtes für die Sicherheit in der Informationstechnik BSI unter www.bsi.de/gshb. Neben allgemeinen Bereichen wie z. B. Personal, Organisation und Gebäude werden auch spezielle Anwendungsbereiche wie z. B. Serverraum, Telearbeit, Unix-System, Netz, Firewall, Telefonanlage ausführlich beschrieben.

Spezielle Gesetzesunterlagen, Informationen und Materialien zum Datenschutz wie z. B. auch eine Orientierungshilfe „Internet“ enthalten die Angebote des Bundes- und der Landesbeauftragten für Datenschutz, die am einfachsten über das **virtuelle Datenschutzbüro unter www.datenschutz.de** zu erreichen sind. Letzteres berät auch zu allgemeinen Fragen oder stellt Kontakt zu einer entsprechenden Stelle her. Das für saarländische Dienststellen relevante Angebot des Landesbeauftragten für Datenschutz ist zu finden unter **www.lfd.saarland.de**.

Außerdem steht der Landesbeauftragte für Datenschutz zu Rückfragen zur Verfügung unter:

Landesbeauftragter für Datenschutz
Fritz-Dobisch-Str. 12, 66111 Saarbrücken
Postfach 10 26 31, 66026 Saarbrücken
Tel.: 0681/94781-36, Fax: 0681/94781-29
eMail: lfd-saar@t-online.de
www.lfd.saarland.de