Datenschutz in der Katholischen Kirche

Sicherheit und Ordnungsgemäßheit kirchlicher Datenverarbeitung

Arbeitshilfe Nr. 501 Stand: Juni 2015

Hinweise zu den Anforderungen an die Schul-EDV bei Anwendung der Schuldatenschutzanordnung[1]

Der Diözesandatenschutzbeauftragte
des Erzbistums Hamburg,
der Bistümer Hildesheim, Osnabrück
und des Bischöflich Münsterschen Offizialats in Vechta i.O.

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

[1] Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft im Erzbistum Hamburg (in der Diözese Hildesheim; in der Diözese Osnabrück; im Offizialatsbezirk Oldenburg)

Hinweise zu den Anforderungen an die Schul-EDV bei Anwendung der Schuldaten-schutzanordnung

Inhalt

Anlagen

Herausgeber:
Der Diözesandatenschutzbeauftragte der norddeutschen Bistümer
Schwachhauser Heerstraße 67 • 28211 Bremen • ☏ 0421 / 16 30 19 25
Internet: http://www.datenschutz-kirche.de
E-Mail: info@datenschutz-katholisch-nord.de

Erscheinungsdatum:
Juni 2015

Situation der elektronischen Datenverarbeitung in der Schule

Die Lehrergewerkschaft VBE hat auf der Grundlage einer von ihr in Auftrag gegeben Forsa-Studie[1] im Jahr 2014 die IT-Ausstattung in den Schulen als „mittelalterlich“ bezeichnet[2]. Dies gelte sowohl für die Ausstattung, wie auch für den Support der Systeme. Bemängelt wurde dabei, dass Schulrechner nur in begrenztem Umfang zur Verfügung stünden, die Lehrkräfte nur zu 57% über geschützte E-Mail-Adressen verfügten und zudem ein technischer IT-Support in 71% von Fachlehrern durchgeführt würde. Auch fehle es an der Vermittlung von Kenntnissen im IT-Bereich für den Unterricht. Berufliche Fortbildung finde hier nicht statt. Die Förderung digitalen Lernens sei in dieser Form nicht möglich[3]. Unabhängig davon, ob diese Feststellungen auch auf unsere Schulen zutreffen oder nicht, wird die Versorgung mit EDV-Systemen für Schulen für die Zukunft immer wichtiger werden. Der Datenschutz will dem nicht entgegenstehen, er legt hingegen Wert darauf, dass die Installation in ordnungsgemäßer Weise und unter Wahrung des Persönlichkeitsrechts des Einzelnen durchgeführt wird.

Die Datenverarbeitung in Schulen kann dabei regelmäßig auf drei Ebenen stattfinden. Neben dem Rechner zur Verwaltung der Schulangelegenheiten (Sekretariatsrechner) gibt es noch die Möglichkeit des Einsatzes privater Systeme der Lehrkräfte nach § 7 SchulDO sowie Computersysteme zur Nutzung durch die Schüler. Alle drei Möglichkeiten sollen hier betrachtet werden.

Rechner zur Verwaltung der Schulangelegenheiten

Zunächst werden Rechner zur Verwaltung der Schulangelegenheiten eingesetzt. Auf ihnen werden die Daten der Schüler, Eltern und eventuell auch Personaldaten der Lehrkräfte verarbeitet. Neben den üblichen Stammdaten (Name, Anschrift, Erreichbarkeit) werden hier auch Daten der Schüler über die Belegung von Kursen, Leistungsbewertungen und in entsprechenden Fällen auch Verhaltensdaten sowie soziale und therapeutische Maßnahmen gespeichert. Von den Eltern werden Funktionen, die sie innerhalb der Schule ausüben, erfasst. Auch allgemeine Informationen, wie die Zusammensetzung der Klassenverbände, die Aufteilung der Lehrer, Stundenpläne und Angebote zu weiteren Veranstaltungen, werden in dieser Datenverarbeitung berücksichtigt.

Die Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft (Schuldatenschutzordnung – SchulDO) gibt eine Reihe von verpflichtenden Vorgaben hierzu. Von den Schülern dürfen nur die in § 1 Abs. 1 SchulDO genannten Daten und mit Einwilligung der Betroffenen zudem die Angaben zu § 1 Abs. 3 erhoben, gespeichert und genutzt werden. Von den Erziehungsberechtigten dürfen nur die Angaben nach § 1 Abs. 2 SchulDO erfasst werden.

[1] Forsa Politik- und Sozialforschung GmbH, IT an Schulen – Ergebnisse einer Repräsentativbefragung von Lehrern in Deutschland, 6. November 2014
[2] VBE-Pressemeldung vom 12.11.2014
[3] VBE-Pressemeldung vom 09.12.2014

Nach § 3a KDO unterliegen die hierzu eingesetzten Verfahren der **Meldepflicht** gegenüber dem Diözesandatenschutzbeauftragten. Sie entfällt nur dann, wenn ein betrieblicher Datenschutzbeauftragter für die Schule bestellt worden ist (§ 3a Abs. 3 Satz 1 KDO) und die Schule ihm in Anwendung von § 21 Abs. 2 KDO die Übersicht nach § 3a Abs. 2 KDO zur Verfügung gestellt hat.

§

§ 3a Abs. 1 KDO Meldepflicht und Verzeichnis

Die in § 1 Abs. 2 genannten Stellen sind verpflichtet, Verfahren automatisierter Verarbeitung vor Inbetriebnahme dem Diözesandatenschutzbeauftragten zu melden.

§ 3a Abs. 3 Satz 1 KDO

Die Meldepflicht entfällt, wenn für die verantwortliche Stelle ein betrieblicher Datenschutzbeauftragter nach § 20 KDO bestellt wurde.

§ 21 Abs. 2 KDO

Dem betrieblichen Datenschutzbeauftragten ist von der verantwortlichen Stelle eine Übersicht nach § 3a Abs. 2 zur Verfügung zu stellen.

Darüber hinaus unterliegen diese Verfahren der **Vorabkontrolle**. Der Grund dafür ist, dass hier auch Daten berücksichtigt werden, die zur Bewertung der Persönlichkeiten der Schüler, einschließlich ihrer Fähigkeiten, Leistungen oder ihres Verhaltens dienen - § 3 Abs. 5 KDO. Die Vorabkontrolle ist regelmäßig von betrieblichen Datenschutzbeauftragten durchzuführen (§ 3 Abs. 6 KDO) und obliegt nur dann, wenn ein solcher nicht bestellt wurde dem Diözesandatenschutzbeauftragten.

§

§ 3 Abs. 5 KDO

Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Eine Vorabkontrolle ist insbesondere durchzuführen, wenn
1. besondere Arten personenbezogener Daten (§ 2 Abs. 10) verarbeitet werden oder
2. die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens, es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

§ 3 Abs. 6 KDO

Zuständig für die Vorabkontrolle ist der betriebliche Datenschutzbeauftragte; soweit kein betrieblicher Datenschutzbeauftragter bestellt ist, ist für die Vorabkontrolle der Diözesandatenschutzbeauftragte zuständig

Soweit der Schulrechner nicht nur von der Schulleitung benutzt wird, sondern auch den Lehrkräften zur Verfügung steht, besteht zudem die Verpflichtung, eine schriftliche Benutzerordnung mit der Festlegung einer Rechteverwaltung hierfür zu erlassen.

§

§ 2 Abs. 2 SchulDO

Für die in den Schulen vorhandenen EDV-Anlagen sollte eine schriftliche Benutzerordnung erlassen werden. In der Benutzerordnung sind die näheren Modalitäten im Umgang mit der EDV-Anlage, die Fragen der Zugriffsberechtigung und die Verantwortlichkeit für die EDV-Anlage, die Weitergabe von Daten an Dritte sowie die Vernichtung eventuell vorhandener Ausdrucke zu regeln. Die Datenverarbeitung der Schulverwaltung ist von der Datenverarbeitung für den Unterrichtsbereich zu trennen.

Neben den stationären EDV-Systemen der Schulverwaltung (Sekretariatsrechner) werden gelegentlich auch noch Notebooks, Laptops und Tablets auf Seiten der Schulleiterinnen und Schulleiter eingesetzt, um diesen ein flexibleres Arbeiten zu ermöglichen. Auf ihnen werden zwar nicht in jedem Fall auch personenbezogene Daten gespeichert. Jedoch ist die Wahrscheinlichkeit hoch, dass dies passiert.

In diesem Fall **müssen** sämtliche auf dem Notebook befindlichen Daten verschlüsselt werden. Nur so kann dem Risiko für die personenbezogenen Daten vor Verlust oder unbefugtem Zugang Rechnung getragen werden. Sollten Sie ein Notebook benutzen, haben Sie also nur die Wahl, die personenbezogenen Informationen zu entfernen bzw. auf diese zu verzichten oder ein professionelles Verschlüsselungsverfahren einzusetzen. Hierzu reicht beispielsweise auch ein Einsatz der Windows BitLocker-Laufwerksverschlüsselung wie sie bei Windows 7 Professional oder Ultimate zur Verfügung steht.

Eine mobile Verbindung mit dem Internet, setzt für alle Systeme voraus, dass eine Personal Firewall und ein Virenschutz installiert sind. Hierbei sollten die Hinweise des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur

- „Sicheren Nutzung von PCs unter Microsoft Windows 7[4]“ (BSI-CS 003) vom 05.09.2013 und zum
- „Management von Schwachstellen und Sicherheitsupdates[5]“ (BSI-CS 093) vom 13.03.2014

beachtet werden.

Private Rechner der Lehrkräfte

Sicher verfügen heute viele Lehrkräfte über private PCs, Notebooks, Tablets oder Smartphones. Dabei ist auch verständlich, dass der Wunsch aufkommt, diese Geräte auch zur eigenen Arbeitserleichterung einzusetzen, zumal ein wesentlicher Teil der Arbeitsleistung von Lehrkräften zu Hause erbracht wird. Die Vorbereitung des Unterrichts und die Verwaltung der Leistungsdaten, der von der Lehrkraft unterrichteten Schüler, lässt sich durch geeignete Pro-

[4] BSI-Veröffentlichungen zur Cyber-Sicherheit, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/anwender/software/BSI-CS_003.html
[5] BSI-Veröffentlichungen zur Cyber-Sicherheit, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/risikomanagement/BSI-CS_093.html

gramme unterstützen. Die Schuldatenschutzanordnung lässt dies inzwischen, in Übereinstimmung mit den gesetzlichen Regelungen in den Bundesländern, zu. Allerdings muss in einem solchen Fall, der Datenschutz durch die Lehrkraft in vollem Umfang gewährleistet werden.

§

§ 7 SchulDO
Verarbeitung personenbezogener Daten
auf privaten Datenverarbeitungsgeräten von Lehrkräften

(1) Lehrkräften der Schule kann mit schriftlicher Genehmigung der Schulleitung gestattet werden, personenbezogene Daten der von ihnen unterrichteten Schüler auf ihren eigenen privaten Datenverarbeitungsanlagen zu verarbeiten.
(2) Das Nähere regelt eine Ausführungsvorschrift zu dieser Anordnung.

Folgende Anforderungen sind nach der Ausführungsvorschrift zu erfüllen:

- Lehrkräfte dürfen nur die Daten der Schüler speichern und verarbeiten, die auch von ihnen unterrichtet werden (Grundsatz der Erforderlichkeit).
- Der Umfang der Datenverarbeitung ist dabei auf den von Ziff. 3.2 der Ausführungsvorschrift zu § 7 SchulDO genannten Datenrahmen zu beschränken.
- Die Daten sind spätestens 1 Jahr nachdem der Schüler nicht mehr von der Lehrkraft unterrichtet wird zu löschen (Ziff. 4.3.).
- Das private EDV-System und die für schulische Aufgaben verwendeten Datenträger sind vor unbefugtem Zugriff zu sichern. Hierbei sollte für die dienstlichen Aufgaben ein eigenes Benutzerprofil auf dem jeweiligen Rechner erstellt werden (Ziff. 4.1.2).
- Internetzugänge sind durch Virenschutzprogramme und Software-Firewalls nach dem aktuellen technischen Stand zu schützen (Ziff. 4.1.2).
- Ein Datenabgleich mit dem Schulverwaltungsrechner ist nur im Umfange des Datenrahmens nach Ziff. 3.2 der Ausführungsvorschriften zulässig.
- Eine Übermittlung dieser Daten an andere Lehrkräfte oder dritte Personen ist nicht zulässig. Die Daten dienen allein der Erfüllung eigener Aufgaben durch die Lehrkraft (Ziff. 4.1).
- Die Lehrkraft hat eine entsprechende Verpflichtungserklärung nach Ziff. 5 abzugeben.

Computersysteme zur Nutzung durch Schüler

Immer häufiger werden Computersysteme zu Unterrichtszwecken eingesetzt. Dabei werden sie nicht nur als Lehrmittel betrachtet, sondern dienen auch zur Vermittlung einer modernen Medienkompetenz, die sich weitgehend im Web 2.0 manifestiert. Für einen Unterricht in dieser Form, werden in der Regel spezielle Lernräume eingerichtet. Soweit sie entsprechend zu Kurszwecken genutzt werden, werden dabei von den Lehrer(innen) vorgegebene Programme genutzt und Webseiten aufgerufen, die zur pädagogisch gezielten Vermittlung von Kompetenz

und Selbstverantwortung im Umgang mit ihnen, erforderlich sind[6]. Dabei werden auch meist keine Daten lebender Personen verarbeitet, so dass hier selten datenschutzrechtliche Probleme auftauchen dürften. Eine Speicherung der Programme und der Daten wird auch in der Regel auf dem Server des Schulnetzwerks erfolgen. Das Land Niedersachsen unterstützt diese Bemühungen in dem ein eigener Bildungsserver als internetgestützte Kooperations- und Lernplattform eingerichtet wurde.

Darüber hinaus stellt sich die Frage, ob diese Lernplattformen den Schülern auch außerhalb des Unterrichts zur Verfügung gestellt werden sollen. In diesem Fall würde beispielsweise die Möglichkeit geschaffen, dass für Referate auch Materialien aus dem Internet genutzt werden können. Dabei sind jedoch eine Reihe wichtiger Punkte zu bedenken:

- Die Schüler(innen) benutzen diese Geräte dann ohne Aufsicht durch eine Lehrkraft.
- Es besteht keine Kontrolle über die aufgesuchten Webseiten. Es können auch gewalttätige, rassistische, pornographische und andere bedenkliche Angebote genutzt werden.
- Es können Urheberrechtsverletzungen begangen werden, die zivilrechtlichen und teilweise auch strafrechtlichen Konsequenzen unterliegen.

Die Schule ist in diesem Fall Diensteanbieter nach § 2 Nr. 1 Telemediengesetz (TMG), während die Schüler als Nutzer nach § 2 Nr. 3 TMG anzusehen sind. Als Rechtsfolge hieraus ergibt sich, dass die Schule die Nutzungsdaten (§ 15 TMG) nur zu Bereitstellungs- und Abrechnungsgründen erfassen darf, aber nicht zur Überwachung der in Anspruch genommenen Telemedien. Andererseits ist auch die Haftung der Schule als Anbieter durch § 7 TMG begrenzt. In Absatz 2 dieser Vorschrift ist deutlich geregelt, dass keine Verpflichtung des Diensteanbieters besteht, die jeweilige Nutzung zu überwachen oder Hinweisen zu strafrechtlichen Tätigkeiten nachzugehen.

§

§ 2 TMG Begriffsbestimmungen

Im Sinne dieses Gesetzes
1. ist Diensteanbieter jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt; bei audiovisuellen Mediendiensten auf Abruf ist Diensteanbieter jede natürliche oder juristische Person, die die Auswahl und Gestaltung der angebotenen Inhalte wirksam kontrolliert,
3. ist Nutzer jede natürliche oder juristische Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen,

§ 7 Allgemeine Grundsätze

(1) Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.
(2) Diensteanbieter im Sinne der §§ 8 bis 10 sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen,

[6] Siehe hierzu auch die vom Landesbeauftragten für den Datenschutz Niedersachsen veröffentlichte Broschüre „Schulen ans Netz – mit Sicherheit“, Kapitel 2, Seite 1 bis 4

die auf eine rechtswidrige Tätigkeit hinweisen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 bis 10 unberührt. Das Fernmeldegeheimnis nach § 88 des Telekommunikationsgesetzes ist zu wahren.

§ 11 TMG Anbieter-Nutzer-Verhältnis

(1) Die Vorschriften dieses Abschnitts gelten nicht für die Erhebung und Verwendung personenbezogener Daten der Nutzer von Telemedien, soweit die Bereitstellung solcher Dienste
1. im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken oder
2. innerhalb von oder zwischen nicht öffentlichen Stellen oder öffentlichen Stellen ausschließlich zur Steuerung von Arbeits- oder Geschäftsprozessen erfolgt.
(2) Nutzer im Sinne dieses Abschnitts ist jede natürliche Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen.
(3) Bei Telemedien, die überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, gelten für die Erhebung und Verwendung personenbezogener Daten der Nutzer nur § 15 Absatz 8 und § 16 Absatz 2 Nummer 4.

§ 15 TMG Nutzungsdaten

(1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind insbesondere
1. Merkmale zur Identifikation des Nutzers,
2. Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und
3. Angaben über die vom Nutzer in Anspruch genommenen Telemedien.

Andererseits ist aber die Haftung für Urheberrechtsverstöße zu berücksichtigen. Werden in unzulässiger Weise Daten kopiert oder heruntergeladen, fällt der Verdacht zunächst auf den Inhaber des Anschlusses, in diesem Fall die Schule. Diese erhält dann auch eine Abmahnung, gegen die sie sich wehren muss. Der Bundesgerichtshof hat jüngst in drei Urteilen[7] festgestellt, dass eine Verantwortlichkeit des Anschlussinhabers bestehe, solange die Nutzer minderjährig sind und ihm eine Aufsichtspflicht nach § 832 Abs. 1 BGB obliege. Verlangt wurde, dass eine Aufklärung des Kindes über Urheberrechte und rechtlich einwandfreies Verhalten im Internet erfolgen müsse und weitere Maßnahmen erfolgen, wenn das Kind ersichtlich diesem Gebot zuwiderhandelt. Wird dies unterlassen, besteht eine Haftung.

§

§ 832 Abs. 1 BGB Haftung des Aufsichtspflichtigen

Wer kraft Gesetzes zur Führung der Aufsicht über eine Person verpflichtet ist, die wegen Minderjährigkeit oder wegen ihres geistigen oder körperlichen Zustands der Beaufsichtigung bedarf, ist zum Ersatz des Schadens verpflichtet, den diese Person einem Dritten widerrechtlich zufügt. Die Ersatzpflicht tritt nicht ein, wenn er seiner Aufsichtspflicht genügt oder wenn der Schaden auch bei gehöriger Aufsichtsführung entstanden sein würde.

§ 62 NSchG Aufsichtspflicht der Schule

(1) Die Lehrkräfte haben die Pflicht, die Schülerinnen und Schüler in der Schule, auf dem Schulgelände, an Haltestellen am Schulgelände und bei Schulveranstaltungen außerhalb der

[7] BGH Urteile vom 11.06.2015, Az.: I ZR 19/14; I ZR 21/14 und I ZR 75/14, siehe Pressemitteilung Nr. 92/2015

Schule zu beaufsichtigen. Die Aufsicht erstreckt sich auch darauf, dass die Schülerinnen und Schüler des Primarbereichs und des Sekundarbereichs I das Schulgrundstück nicht unbefugt verlassen.
(2) Geeignete Mitarbeiterinnen und Mitarbeiter der Schule (§ 53 Satz 1), das Betreuungspersonal (§ 53 Satz 2) sowie geeignete Erziehungsberechtigte können mit der Wahrnehmung von Aufsichtspflichten betraut werden. Auch geeignete Schülerinnen und Schüler können damit betraut werden, wenn das Einverständnis ihrer Erziehungsberechtigten vorliegt.

Nicht umsonst verlangt daher § 2 Abs. 2 den Erlass einer schriftlichen Benutzerordnung für die vorhandenen EDV-Anlagen. Dabei ist folgendes zu beachten: Die Schule ist nicht verpflichtet, ihre EDV-Anlage zur allgemeinen Benutzung zur Verfügung zu stellen. Tut sie es doch, kann und darf sie Regeln dafür aufstellen, welche Nutzung erlaubt sein soll und welche Maßnahmen hierbei zu beachten sind. Die Nutzungsordnung ist insoweit die für Computerräume geltende Hausordnung. Ein Muster hierfür ist in der Anlage 1 dargestellt. Darüber hinaus sollten sich alle Schüler(innen), die als Nutzer zugelassen werden möchten, mit dieser Ordnung einverstanden erklären. Das entsprechende Muster ist als Anlage 2 beigefügt.

Trennung der Systeme

§

§ 2 Abs. 2 Satz 3 SchulDO
Technische und organisatorische Maßnahmen

Die Datenverarbeitung der Schulverwaltung ist von der Datenverarbeitung für den Unterrichtsbereich zu trennen.

Eine mögliche Verbindung des Schulrechners mit Systemen, die von den Schülern benutzt werden können, ist untersagt. Gemeint ist hiermit eine physikalische Trennung zwischen Verwaltungsnetzwerk und dem pädagogischen Netzwerk. Der Grund hierfür liegt in folgenden Überlegungen:

- Die Schülerinnen/Schüler haben keine Berechtigung, die Daten von anderen Schülern, Lehrern oder Eltern einzusehen.
- Es darf zudem keine Möglichkeit bestehen, sich vorab über Prüfungsaufgaben zu informieren.
- Selbstverständlich dürfen die Daten nicht durch Schülerinnen/Schüler verändert oder gar gelöscht werden!
- Gerade Jugendliche verfügen oft über erhebliche Hacker-Fähigkeiten.
- Die Gefährdung durch Viren und andere Schadprogramme wird hierdurch erheblich erhöht, vor allem beim Einsatz von externen Speichermedien (z.B. Sticks)

Eine vollständige Trennung durch zwei völlig selbständige Systeme ist dabei die einfachste und auch auf Dauer sicherste Methode. Aber auch eine Trennung durch technische Geräte ist heute möglich. Sie erfordert jedoch eine umfangreiche Konzeption und eine ständige Überprüfung / Wartung. Die im Grundschutzkatalog im Kapitel M 5.61 (Geeignete physikalische

Segmentierung) veröffentlichten Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik sind hier zu beachten.

Schutz vor unberechtigtem Zugriff

Die nachfolgenden Ausführungen sind auf alle Computersysteme anzuwenden. Sowohl beim Sekretariatsrechner, wie auch bei Systemen, die für Lehrer und Schüler zur Verfügung stehen, einschließlich der dienstlich genutzten Privatrechner sind durch technisch-organisatorische Maßnahmen, Sicherungen für ordnungsgemäße Nutzungen erforderlich. Hier gelten §§ 2 Abs. 1 SchulDO, 6 KDO und IV. KDO-DVO [8]

§

§ 2 Abs. 1 SchulDO
Technische und organisatorische Maßnahmen

Die in den Schulen gespeicherten personenbezogenen Daten dürfen nur denen zugänglich gemacht werden, die die Daten zur Erfüllung ihres dienstlichen Auftrags benötigen. Sie sind vor Unbefugten zu sichern und in abschließbaren Schränken aufzubewahren. Zugangsberechtigt sind außer der Schulsekretärin und dem Schulleiter bzw. Schulträger nur die jeweils für den Schüler zuständigen Lehrer.

Die Daten der Mitarbeiter, Schüler und Erziehungsberechtigten sind vor dem Zugriff Unbefugter zu schützen. Dafür sind Vorkehrungen sowohl in technischer, wie organisatorischer Hinsicht zu treffen. Die Verantwortlichkeit hierfür liegt bei der Schulleitung.

1. Akten in Papierform (Personalakten, Schülerakten) sowie Ausdrucke der EDV-Dateien sind in verschließbaren Aktenschränken aufzubewahren, die nach Dienstschluss in jedem Fall abzuschließen sind. Bei kurzfristiger Abwesenheit der zugriffsberechtigten Person reicht im Allgemeinen ein Abschließen des Raumes bis zur Rückkehr aus.

2. Das EDV-System muss mit einer Zugangssicherung ausgestattet sein. Für eine Benutzerin oder einen Benutzer muss ein Anwenderkonto, ohne Administratorrechte angelegt werden, in dem sie sich mit einem Login und einem Passwort identifizieren müssen. Die Anlage eines „Gastkontos“, das einen Zugriff ohne Identifizierung ermöglicht, ist auszuschließen. Voraussetzung hierfür ist, dass das verwendete Betriebssystem eine solche Zugangssicherung anbietet. Für Microsoft-Betriebssysteme ab Windows NT ist dies Standard.

Rechteverwaltung / Passwortschutz

Für die Passwortgestaltung und -länge gibt es allgemein anerkannte Regeln. Nach dem heutigen Stand gelten mindestens achtstellige Passwörter als relativ sicher. Dies gilt jedoch nur, wenn sie aus einer Kombination von Buchstaben, Zahlen und Sonderzeichen gebildet werden. Sie sollten den Benutzerinnen und Benutzern die Sinnhaftigkeit dieser Maßnahme deutlich machen. Dies fällt nicht immer leicht. Sicherlich ist es schwierig, sich komplizierte Passwörter

[8] Siehe Anlage 4

zu merken. Es besteht das Risiko, dass diese aufgeschrieben und in der Nähe des EDV-Systems aufbewahrt werden, so dass auch Unbefugte diese finden könnten.

Passwörter sollten – auch in Vertretungsfällen – auf keinen Fall weitergegeben werden. Bei längerfristiger Abwesenheit eines Mitarbeiters (z.B. im Krankheitsfall) sollte die Zugriffsberechtigung zugunsten des Vertreters solange geändert werden. Hat der Mitarbeiter den Eindruck, dass sein Passwort bekannt geworden ist, hat er es unverzüglich zu ändern.

Die Zugriffsberechtigung sollte sich nicht nur auf die rechtliche Möglichkeit des Zugriffs erstrecken, sondern auch auf die technischen Anforderungen. Wer darf die gespeicherten Daten nur sehen, wer darf sie auch anlegen, bearbeiten und verändern, sie sperren oder gar löschen? Auch diese Einschränkungen haben erhebliche Auswirkungen auf die Richtigkeit und Zuverlässigkeit des Datenbestandes. Eine klare Regelung sorgt in diesem Bereich für eine ordnungsgemäße Verwaltung.

Geschlossene Laufwerke

PC mit offenen Disketten- und CD-ROM/DVD-Laufwerken und unversperrten USB-Schnittstellen ermöglichen ohne weiteres den Zugang für Unbefugte. Es ist dann leicht möglich, die installierten Zugangssicherungen (bspw. des Betriebssystems) zu umgehen. Entsprechende Programme, um Passwörter auszulesen, zu manipulieren oder auszuschalten, sind im Internet frei erhältlich. Solche Sicherheitslücken müssen durch technische Maßnahmen möglichst ausgeschlossen werden. Dies kann z. B. dadurch erreicht werden, dass vorhandene Laufwerke im BIOS abgeschaltet werden (natürlich muss der Zugang zum BIOS dann passwortgeschützt werden). Es gibt zudem spezielle Programme, die den Zugang zu den Laufwerken schützen. Die richtigen Einstellungen im Betriebssystem können den Zugriff auf die Laufwerke durch Unbefugte ebenfalls unterbinden.

Sicherstellung eines reibungslosen Betriebs

§

§ 6 KDO
Technische und organisatorische Maßnahmen

Kirchliche Stellen im Geltungsbereich des § 1 Abs. 2, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieser Anordnung, insbesondere die in der Anlage zu dieser Anordnung genannten Anforderungen zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

EDV-Systeme müssen gewartet, d. h. administriert werden. Es müssen Updates für das Betriebssystem und die Anwendungsprogramme eingepflegt werden. Allein die Zahl der Sicherheitsupdates, die meist wöchentlich veröffentlicht werden, macht deutlich, dass nur hierdurch ein reibungsloser und ordnungsgemäßer Betrieb zu gewährleisten ist. Eine Forsa-Repräsentativ-Erhebung, die im Auftrag der Gewerkschaft VBE durchgeführt wurde, ergab, dass nicht

einmal die Hälfte der Schulen über einen IT-Support verfügen![9] Die insoweit bessere Lösung, diese Aufgabe den Administratoren der Verwaltung des Schulträgers zu übertragen, wird häufig durch die Einbindung von Lehrkräften oder sogar Eltern oder Schüler ersetzt. Dabei haben 89% der Lehrer bei der Forsa-Befragung angegeben, sich die notwendigen Kenntnisse für den Einsatz von digitalem Unterrichtsmaterial privat angeeignet zu haben.[10]

§ 6 KDO verlangt, dass Sie diese Personen auswählen und Ihnen die Aufgabe detailliert zuweisen. Ferner müssen Sie jederzeit wissen, wann und welche Veränderungen an den Programmen vorgenommen wurden. Soweit die Theorie. In der schulischen Praxis erfolgt die Administration zumeist völlig kontrollfrei. Das hat in der Regel den Grund, dass Schulleiterinnen und Schulleiter selbst nicht über ausreichende technische Kenntnisse verfügen und froh darüber sind, dass ihnen diese Arbeit abgenommen wird. Aber Sie sind und bleiben für die ordnungsgemäße Datenverarbeitung verantwortlich.

→ Wenn Sie Ihr Schulverwaltungssystem nicht selbst administrieren, müssen Sie Folgendes beachten: Unabhängig davon, wer den oder die Schulverwaltungsrechner administriert: Sie als Schulleiterin oder Schulleiter erteilen den Auftrag hierfür.

Auch wenn die Hardware und die Programme vom Schulträger bezahlt werden, hat dieser hinsichtlich des Umganges mit der EDV keine freie Entscheidungskompetenz. Die Schule als datenverarbeitende Stelle wird von Ihnen verantwortlich vertreten. Damit sind nur Sie entscheidungsbefugt. Dies bedeutet, dass Änderungen am EDV-System vorher mit Ihnen zu besprechen sind und Sie die Genehmigung erteilen müssen, ob diese Änderungen vorgenommen werden dürfen.

Überlassen Sie die Administration einer Lehrkraft oder dem Administrator ihres Schulträgers, müssen Sie die Person hierzu schriftlich ermächtigen. Sie müssen dabei festlegen, dass alle Änderungen an der Hardware und an den Programmen zu dokumentieren sind. Nur auf diese Weise erfüllen Sie die Vorgabe des § 6 KDO.

Regelmäßige Datensicherung

Viele Schulverwaltungen scheinen sich wegen der Gefahr von Datenverlusten wenig Sorgen zu machen. Häufig werden die in den Schulverwaltungsprogrammen gespeicherten Informationen entweder überhaupt nicht oder nur sporadisch gesichert.

Datensicherungen sind aber erforderlich, um Datenverlusten im Falle des Ausfalls des Systems durch technische Defekte oder des Diebstahls des Rechners und einer Vernichtung durch Brand- oder Wasserschäden vorzubeugen. Die Abstände, in denen Datensicherungen vorge-

[9] Forsa Politik- und Sozialforschung GmbH, IT an Schulen – Ergebnisse einer Repräsentativbefragung von Lehrern in Deutschland, 6. November 2014, veröffentlicht auf der Webseite des VBE, Pressemeldung vom 12.11.2014
[10] Seite 12 der Forsa-Studie

nommen werden sollten, sind dabei abhängig von der Intensität der Änderungen der Datenbestände. So kann es beispielsweise in einer Schule mit wenigen Schülerinnen und Schüler ausreichen, eine Datensicherung nur einmal wöchentlich durchzuführen.

Wichtig ist, dass die Sicherungsmedien nicht in der Nähe des Rechners aufbewahrt werden. Die Datensicherungsmedien sollten in jedem Fall brandgeschützt in einem anderen Raum gelagert werden. Bei der Aufbewahrung sollte die Verwendung eines Tresors oder eines speziellen Datensicherungsschrankes erwogen werden. In jedem Fall ist ein abschließbarer Schrank vorzusehen.

Anschluss an das Internet

Aus den gleichen Gründen sollte auch der Verwaltungsrechner keine unmittelbare Verbindung zum Internet haben. Soweit ein Internetzugang für die Arbeit der Schulverwaltung überhaupt erforderlich ist, kann hierfür ein spezieller Rechner eingesetzt werden, auf dem keine personenbezogenen Daten verarbeitet werden und von dem aus auch kein Zugriff auf den Rechner der Schulverwaltung möglich ist.

→ Rechner mit Internetzugang sind mindestens mit einer Firewall und einem Virenschutzprogramm zu sichern.

Für die pädagogische Arbeit der Lehrer steht meistens ein dienstlicher Computer mit Internetzugang zur Verfügung. Auch dieser ist vom Verwaltungsrechner technisch zu trennen und darf nicht in einem Netzwerk mit ihm verbunden sein.

Verarbeitung von Personaldaten

Allgemeine datenschutzrechtliche Anforderungen
Personenbezogene Daten fallen bei der Nutzung dieser technisch unterstützten Verfahren als Inhaltsdaten (Personaldaten bzw. Personalaktendaten) und als Protokolldaten (mit besonderer Zweckbindung) an.

Für den Umgang mit diesen Daten gelten die folgenden allgemeinen Grundsätze:

1. Personenbezogene Daten der Beschäftigten dürfen in technikgestützten Verfahren nur in dem Umfang gespeichert, verändert und genutzt werden, in dem dies rechtlich zulässig und im Rahmen der festgelegten Zwecke zur Durchführung der jeweiligen Stelle obliegenden personalwirtschaftlichen, organisatorischen und sozialen Aufgaben erforderlich ist (Grundsatz der Zulässigkeit, Zweckbindung und Erforderlichkeit, § 10a Abs. 1 KDO).
2. In einem Berechtigungskonzept ist festzulegen, welche Stellen und/oder Funktionsträgerinnen oder Funktionsträger im Rahmen der ihnen übertragenen Aufgaben für welche Zwecke und in welcher Form (lesend/verändernd) befugt sind, auf Daten zuzugreifen oder Auswertungen vorzunehmen. Das Berechtigungskonzept ist fortzuschreiben und laufend an organisatorische Veränderungen anzupassen.

3. Es ist schon im Vorfeld bei der Auswahl und Gestaltung der automatisierten Verfahren darauf hinzuwirken, dass keine oder möglichst wenig personenbezogene Daten verarbeitet werden (Grundsatz der Datenvermeidung und Datensparsamkeit, § 2a KDO).
4. Die Betroffenen sind über ihren persönlichen Datenbestand, die Zwecke der Verarbeitung und Zugriffsberechtigungen zu unterrichten. Ihre Rechte auf Auskunft, Sperrung und Löschung sind zu wahren. (Transparenzgebot und Betroffenenrechte, § 13 KDO).
5. Arbeits- und dienstrechtliche Entscheidungen, die für die Betroffenen eine rechtliche Folge nach sich ziehen oder sie erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dient (Verbot der automatisierten Einzelentscheidung).
6. Zulässige dienststellenübergreifende Auswertungen der in den Verfahren verarbeiteten Personaldaten sollten soweit möglich anonym oder pseudonym erfolgen; dies gilt nicht für Auswertungen, Abgleiche oder Zusammenführungen, die sich auf die in der Anlage aufgeführten Merkmale (Informationen zur dienstlichen Funktion und Erreichbarkeit = sogenannte Funktionsträgerdaten) beschränken.
7. Die Sicherungsziele Vertraulichkeit, Integrität, Authentizität und Revisionsfähigkeit sind - ausgerichtet am Schutzbedarf der Daten - durch geeignete technisch-organisatorische Maßnahmen zu gewährleisten; das Grundschutz-Handbuch des Bundesamtes für Sicherheit in der Informationstechnik BSI gibt dazu zahlreiche Hilfestellungen.
8. Protokolldaten von Anwenderinnen und Anwendern sowie Administratorinnen und Administratoren, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs gespeichert werden, dürfen grundsätzlich nicht für andere Zwecke, insbesondere nicht für eine Verhaltens- und Leistungskontrolle, verarbeitet werden. Die Zweckbindung muss daher technisch und organisatorisch (z. B. durch Dienstanweisung) sichergestellt werden. Für Art, Umfang und Aufbewahrung der Protokollierung gilt der Grundsatz der Erforderlichkeit. Soweit technisch möglich und ausreichend sollte auf personenbezogene Daten verzichtet werden. Die Beteiligungsrechte des Personalrates sind zu beachten.
9. Die Verfahren sind in inhaltlicher und technischer Hinsicht ausreichend und nachvollziehbar zu dokumentieren.
10. Die betrieblichen Beauftragten für den Datenschutz sind bei der Entwicklung und Implementierung der Verfahren frühzeitig zu beteiligen.
11. Um die Akzeptanz zu fördern, wird empfohlen, über Einführung und Anwendung der Verfahren eine Dienstvereinbarung mit dem Personalrat abzuschließen, in der insbesondere die Fragen der Zugriffsberechtigungen, der Zulässigkeit und Zweckbestimmung von Auswertungen und die Durchführung von Kontrollen für alle Beteiligten eindeutig und klar geregelt werden. Soweit die Verfahren geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen, sind die Mitbestimmungs- bzw. Mitwirkungsrechte der Personalvertretung zu berücksichtigen.

Bestellung eines betrieblichen Datenschutzbeauftragten

§

§ 2a Abs. 1 SchulDO
Betrieblicher Beauftragter für den Datenschutz

Für die Schulen kann ein betrieblicher Beauftragter für den Datenschutz bestellt werden. Mehrere Schulen können gemeinsam einen betrieblichen Datenschutzbeauftragten bestellen. Die Bestellung muss schriftlich erfolgen.

Mit der Bedeutung der elektronischen Datenverarbeitung sind auch die Risiken des Technikeinsatzes gewachsen. Zudem besteht eine zunehmende Tendenz, sich allein auf die Computertechnik zu verlassen und die klassische Aktenführung ganz einzustellen. Andererseits besteht häufig große Unsicherheit hinsichtlich der datenschutzrechtlichen Anforderungen bei der Ausgestaltung der eingesetzten Systeme. Zudem bestehen oftmals „gewachsene EDV-Landschaften“, die im Laufe der Jahre mehr und mehr verändert und ausgeweitet wurden, ohne dass jemals ein schlüssiges Gesamtkonzept hierfür erstellt wurde.

Solange alles, bis auf kleinere Probleme, reibungslos funktioniert macht sich auch niemand ernsthaft Gedanken um die Gefahren, die der Vertraulichkeit, Integrität und Verfügbarkeit der Daten drohen. Wesentliche organisatorische Maßnahmen, wie das Vorliegen einer schriftlichen Benutzerordnung (§ 2 Abs. 2 SchulDO)[11], die Verpflichtung der an der Datenverarbeitung Beteiligten auf das Datengeheimnis (§ 4 KDO) oder die Meldung der eingesetzten Verfahren an den Diözesandatenschutzbeauftragten (§ 3a KDO) unterbleiben. Der Schulleiter ist verantwortlich, hat aber keine Zeit, sich hierum zu kümmern. Aus diesem Grunde gibt § 2a SchulDO die Möglichkeit mit der Bestellung eines betrieblichen Datenschutzbeauftragten jemanden dafür zu gewinnen, gerade diese wichtigen Aspekte in den Blick zu nehmen und die Schulleitung bei der Wahrnehmung dieser Aufgaben zu entlasten. Jede größere Schule sollte daher ernsthaft überlegen, ob sie in Wahrnehmung ihrer Verantwortung für das informationelle Selbstbestimmungsrecht der Schüler, Eltern und Lehrer allein oder auch mit anderen Schulen gemeinsam, einen betrieblichen Datenschutzbeauftragten bestellen sollte.

Nach § 2a SchulDO kann ein betrieblicher Datenschutzbeauftragter bestellt werden. Diese Vorschrift ist das speziellere Recht und geht somit dem allgemeinen Recht, wie es in § 20 KDO seinen Ausdruck gefunden hat, vor. Nach der Anfang 2014 vorgenommenen Neufassung der KDO soll ein betrieblicher Datenschutzbeauftragter bestellt werden, wenn mehr als 10 Personen mit der automatisierten Verarbeitung personenbezogener Daten befasst sind (§ 20 Abs. 2 KDO). Die Abweichung in der Schuldatenschutzordnung hat jedoch nicht den Grund, die Schulen besser stellen zu wollen. Vielmehr ist dieser Unterschied nur daraus zu erklären, dass die Bestimmung des § 2a SchulDO in einer Zeit geschaffen wurde, zu der auch die KDO insoweit eine reine „kann“-Regelung enthielt (2008). Die insoweit notwendige Änderung der Schuldatenschutzordnung ist bisher nicht erfolgt.

[11] In der hier wiedergegebenen Anlage 1 ist ein Muster für eine „Nutzungsordnung für die Informations- und Kommunikationstechnik an Schulen“ abgedruckt. Sie ist auch auf der Webseite ‚http://www.datenschutz-kirche.de/schulen‘ veröffentlicht.

Zu Bedenken ist auch, dass im Land Niedersachsen alle Ämter, die personenbezogene Daten automatisiert verarbeiten, einen behördlichen Datenschutzbeauftragten zu bestellen haben (§ 8a Abs. 1 NDSG). Hierbei werden auch öffentliche Schulen in staatlicher Trägerschaft einbezogen. Die Schulbehörden des Landes gehen also davon aus, dass ein Datenschutzbeauftragter bestellt worden ist. Ein Unterschied zwischen staatlichem und kirchlichem Recht auf einem derart wichtigen Gebiet war und ist nicht gewollt. Daher habe ich den Bistümern eine Änderung des § 2a Abs. 1 SchulDO vorgeschlagen.

→ Solange eine Änderung nicht erfolgt ist, sollten die Schulen freiwillig einen Betriebsbeauftragten für ihren Bereich bestellen!

Er hat die Aufgaben, die in § 21 KDO festgelegt sind.

- Er wirkt auf die Einhaltung der Schuldatenschutzanordnung und der Anordnung über den kirchlichen Datenschutz hin.
- Er überwacht die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme
- Er macht die mit der Verarbeitung beauftragten Personen mit den Vorschriften des Datenschutzes vertraut.
- Die Meldungen nach § 3a KDO sind ihm zur Verfügung zu stellen. Das Verzeichnis der Datenverarbeitungen nach § 3a Abs. 4 KDO ist von ihm jedem, der ein berechtigtes Interesse nachweist, verfügbar zu machen.
- Er arbeitet mit dem Diözesandatenschutzbeauftragten zusammen.
- Darüber hinaus, führt er nach § 3 Abs. 5 und 6 KDO die Vorabkontrolle für die in der KDO festgelegten Verfahren durch.

Er nimmt als besonderer Beauftragter den Datenschutz in den Blick und trägt dazu bei, dass die Anforderungen aus § 6 KDO besser erfüllt werden können. Insoweit unterstützt er die Schulleitung bei der Erfüllung ihrer Verpflichtungen.

Für mehrere Schulen kann ein gemeinsamer Datenschutzbeauftragter bestellt werden. Es macht durchaus Sinn, wenn zum Beispiel allgemeinbildende Schulen, die gleichartige Probleme lösen müssen, jemanden einstellen, der gerade hier fachkundig ist und zudem die Bedingungen an unterschiedlichen Stellen kennt. Hier sollte eine Absprache mit den Schulträgern erfolgen.

– Anlage 1 –

Nutzungsordnung

für die Informations- und Kommunikationstechnik an der ……..-Schule in ……[12]

A. Allgemeines

Nachfolgende Regelung gilt für die Benutzung der schulischen Informations- und Kommunikationstechnik (z.B. von Computereinrichtungen, Internet, E-Mail) durch Schülerinnen und Schüler und die sonstigen Angehörigen der Schule (z. B. Lehrer, Hausmeister) im Rahmen des Unterrichts, der Gremienarbeit sowie von Arbeitsgemeinschaften und weiteren schulischen Angeboten und Veranstaltungen außerhalb des Unterrichts. Sie gilt nicht für die rechnergestützte Schulverwaltung.

Die Schule gibt sich für den Umgang mit diesem Medium die folgende Nutzungsordnung. Dabei gilt Teil B für jede Nutzung der Schulcomputer, Teil C ergänzt Teil B in Bezug auf die Nutzung außerhalb des Unterrichtes. Die Nutzung der Informations- und Kommunikationstechnik der Schule ist nur unter Einhaltung dieser Nutzungsordnung zulässig, die Bestandteil der Hausordnung bzw. der Schulverfassung ist.

B. Regeln für jede Nutzung

Weisungsberechtigung

Weisungsberechtigt sind die Lehrer, die Schulleitung, die Systembetreuer und sonstige mit dieser Aufgabe beauftragte Personen.

Passwörter

Alle Schülerinnen und Schüler erhalten individuelle Nutzerkennungen mit Passwort, mit denen sie sich an den Geräten der Informations- und Kommunikationstechnik der Schule anmelden können. Das nur dem Benutzer bekannte Passwort sollte mindestens 8 Stellen umfassen, nicht leicht zu erraten sein und eine beschränkte Gültigkeit für die Dauer eines Schulhalbjahres haben. Das Passwort ist vertraulich zu behandeln und gegebenenfalls zu ändern, falls die Gefahr besteht, dass es Unbefugten zur Kenntnis gelangt ist. Vor der ersten Benutzung muss das eigene Benutzerkonto, der Account, freigeschaltet werden. Ohne individuelles Passwort ist keine Arbeit am Computer möglich. Nach Beendigung der Nutzung ist eine Abmeldung vorzunehmen.

[12] *Dieses Muster kann von jeder Schule benutzt und entsprechend den jeweiligen Anforderungen und Gegebenheiten modifiziert werden.*

Die Nutzer sind für die unter ihrer Nutzerkennung erfolgten Handlungen verantwortlich. Deshalb muss das Passwort vertraulich gehalten werden. Das Arbeiten unter einem fremden Benutzerkonto/Passwort ist unzulässig.

Verbotene Nutzungen

Die gesetzlichen Bestimmungen insbesondere des Strafrechts, Urheberrechts und des Jugendschutzrechts sind zu beachten. Es ist verboten, pornographische, gewaltverherrlichende oder rassistische Inhalte aufzurufen oder zu versenden. Werden solche Inhalte versehentlich aufgerufen, ist die Anwendung zu schließen und der Aufsichtsperson Mitteilung zu machen.

Eine private Nutzung ist nicht zulässig.

Datenschutz und Datensicherheit

Die Schule ist in Wahrnehmung ihrer Aufsichtspflicht berechtigt, den Datenverkehr zu speichern und zu kontrollieren. Diese Daten werden in der Regel nach einem Monat, spätestens jedoch zu Beginn eines jeden neuen Schuljahres gelöscht. Dies gilt nicht, wenn Tatsachen den Verdacht eines schwerwiegenden Missbrauches der schulischen Computer begründen.

Die Schule wird von ihren Einsichtsrechten nur in Fällen des Verdachts von Missbrauch und durch verdachtsunabhängige Stichproben Gebrauch machen.

Die Schule und ihre Nutzer sind berechtigt, die vorhandene Software für Ausbildungszwecke zu nutzen. Eine Nutzung für gewerbliche Zwecke sowie eine Vervielfältigung oder Veräußerung ist nicht gestattet.

Alle auf den Arbeitsstationen und im Netz befindlichen Daten (einschließlich persönlicher Daten) unterliegen dem Zugriff der Netzadministratoren.

Im Netz sollen der Systembereich sowie die persönlichen Arbeitsbereiche durch Passwörter gegen unbefugten Zugriff gesichert werden.

Eine Geheimhaltung von Daten, die über das Internet oder per E-Mail übertragen werden, kann grundsätzlich nicht gewährleistet werden. Die Bereitstellung von Informationen im Internet kommt damit einer Veröffentlichung gleich. Die besondere Funktionalität von Suchmaschinen erlaubt es, solche Daten in unterschiedlichen Angeboten zu finden und gegebenenfalls zu einem Persönlichkeitsprofil zu verknüpfen. Es besteht kein Rechtsanspruch gegenüber der Schule auf Schutz solcher Daten vor unbefugten Zugriffen. Insbesondere ist eine E-Mail aus technischen Gründen mit einer Postkarte gleichzusetzen, die von jedem gelesen, verfälscht oder gelöscht werden kann.

Eingriffe in die Hard- und Softwareinstallation

Veränderungen der Installation und Konfiguration der Arbeitsstationen und des Netzwerkes sowie Manipulationen an der Hard- und Softwareausstattung sowie das Verändern von Zugriffsrechten und das Kopieren von Programmen sind grundsätzlich untersagt. Fremdgeräte (z. B. Peripheriegeräte wie externe Laufwerke, Scanner und Digitalkameras) dürfen nur mit Zustimmung des Aufsichtsführenden an Computer oder an das Netzwerk angeschlossen werden. Unnötiges Datenaufkommen durch Laden und Versenden von großen Dateien (z.B. Grafiken) aus dem Internet ist zu vermeiden. Sollte ein Nutzer unberechtigt größere Datenmengen in seinem Arbeitsbereich ablegen, ist die Schule berechtigt, diese Daten zu löschen.

Schutz der Geräte

Die Bedienung der Hard- und Software hat entsprechend den Instruktionen zu erfolgen. Störungen oder Schäden sind sofort der für die Computernutzung verantwortlichen Person zu melden. Wer schuldhaft Schäden verursacht, hat diese zu ersetzen.

Die Tastaturen sind durch Schmutz und Flüssigkeiten besonders gefährdet. Deshalb sind während der Nutzung der Schulcomputer Essen und Trinken verboten.

Nutzung von Informationen aus dem Internet

Der Internet-Zugang soll grundsätzlich nur für schulische Zwecke genutzt werden. Als schulisch ist auch ein elektronischer Informationsaustausch anzusehen, der unter Berücksichtigung seines Inhalts und des Adressatenkreises mit der schulischen Arbeit im Zusammenhang steht. Das Herunterladen von Anwendungen ist nur mit Einwilligung der Schule zulässig.

Die Schule ist nicht für den Inhalt der über ihren Zugang abrufbaren Angebote Dritter im Internet verantwortlich.

Im Namen der Schule dürfen weder Vertragsverhältnisse eingegangen noch ohne Erlaubnis kostenpflichtige Dienste im Internet benutzt werden.

Bei der Weiterverarbeitung von Daten aus dem Internet sind insbesondere Urheber- oder Nutzungsrechte zu beachten.

Versenden von Informationen in das Internet, Homepage, Gästebuch, Foren, Chats

Werden Informationen unter dem Absendernamen der Schule in das Internet versandt, geschieht das unter Beachtung der allgemein anerkannten Umgangsformen. Der Internet-Zugang und die Mail-Funktion dürfen nicht zur Verbreitung von Informationen verwendet werden, die dem Ansehen der Schule Schaden zufügen könnten.

Die Veröffentlichung von Internetseiten der Schule bedarf der Genehmigung durch die Schulleitung.

Um Haftungsfragen auszuschließen, werden gegebenenfalls Gästebücher, Foren und Chats durch dafür bestimmte Moderatoren überwacht.

Für fremde Inhalte ist insbesondere das Urheberrecht zu beachten. So dürfen zum Beispiel digitalisierte Texte, Bilder und andere Materialien nur mit Erlaubnis der Urheber in eigenen Internetseiten verwandt werden. Der Urheber ist zu nennen, wenn dieser es wünscht.

Das Recht am eigenen Bild ist zu beachten. Die Veröffentlichung von Fotos und Schülermaterialien im Internet ist nur gestattet mit der Genehmigung der Schülerinnen und Schüler sowie im Falle der Minderjährigkeit ihrer Erziehungsberechtigten.

Das Kopieren von Texten aus erhaltenen Briefen oder E-Mails bedarf der Zustimmung des Absenders.

Oberster Grundsatz ist die Achtung der Persönlichkeitsrechte anderer Personen. Diskriminierungen, persönliche Angriffe, Unterstellungen und Verleumdungen können neben dem Entzug der Nutzungsberechtigung auch zu einer strafrechtlichen Verfolgung führen.

Die Kommunikation in jeglichen Netzdiensten (E-Mail, Chat, Newsgroups usw.) unter Verwendung von anderen Namen als dem eigenen ist verboten. Als Aliasnamen sind nur die zugelassenen bzw. eingetragenen Aliasnamen zu verwenden.

Das Ausfüllen von Online-Formularen ist ohne ausdrückliche Aufforderung der aufsichtführenden Lehrperson untersagt.

C. Ergänzende Regeln für die Nutzung außerhalb des Unterrichtes

Nutzungsberechtigung, Benutzerausweis

Außerhalb des Unterrichts kann im Rahmen der medienpädagogischen Arbeit ein Nutzungsrecht gewährt werden. Die Entscheidung darüber und darüber, welche Dienste genutzt werden können, trifft die Schule unter Beteiligung der schulischen Gremien.

Alle Nutzer werden über diese Nutzungsordnung unterrichtet. Die Schülerinnen und Schüler sowie im Falle der Minderjährigkeit ihre Erziehungsberechtigten, versichern durch ihre Unterschrift (siehe Anlage), dass sie diese Ordnung anerkennen. Dies ist Voraussetzung für die Nutzung.

Mit ihrer Zulassung wird den Schülerinnen und Schülern ein Benutzerausweis ausgestellt.[13]

[13] Auf die Ausstellung von Benutzerausweisen kann (z.B. bei kleinen Schulen) verzichtet werden, wenn anderweitige Aufsichtsmöglichkeiten ausreichend sind.

Eigenes Arbeiten am Computer außerhalb des Unterrichts ist für Schülerinnen und Schüler nur unter Aufsicht und nur mit Benutzerausweis möglich.

Aufsichtspersonen

Die Schule hat eine weisungsberechtigte Aufsicht sicherzustellen, die im Aufsichtsplan einzutragen ist. Dazu können neben Lehrkräften und sonstigen Bediensteten der Schule auch Eltern und für diese Aufgabe geeignete Schülerinnen und Schüler eingesetzt werden.

D. Schlussvorschriften

Diese Nutzungsordnung ist Bestandteil der jeweils gültigen Hausordnung und tritt am Tage nach ihrer Bekanntgabe durch Aushang in der Schule in Kraft.

Einmal zu jedem Schuljahresbeginn findet eine Nutzerbelehrung statt, die im Klassenbuch protokolliert wird.

Nutzer, die unbefugt Software von den Arbeitsstationen oder aus dem Netz kopieren oder verbotene Inhalte nutzen, machen sich strafbar und können zivil- oder strafrechtlich verfolgt werden.

Zuwiderhandlungen gegen diese Nutzungsordnung können neben dem Entzug der Nutzungsberechtigung schulordnungsrechtliche Maßnahmen zur Folge haben.

Diese Nutzungsordnung wurde in der Schulkonferenz vom ..... beschlossen.

– Anlage 2 –

Erklärung:

Am _____ wurde ich in die Nutzungsordnung zur Internet-Nutzung eingewiesen. Ein Exemplar dieser Nutzungsordnung wurde mir ausgehändigt. Mit den festgelegten Regeln bin ich einverstanden.

_____ _____

Name und Klasse/Kurs Unterschrift der Schülerin/des Schülers

_____

Ort / Datum

_____

(Bei Minderjährigen Unterschrift der/des Erziehungsberechtigten)

– Anlage 3 –

Bestellung zum betrieblichen Datenschutzbeauftragten

gemäß § 20 der Anordnung über den kirchlichen Datenschutz - KDO

Sehr geehrte(r) Herr/Frau _____

Mit Wirkung vom _____ bestelle ich Sie zur/zum betrieblichen Datenschutzbeauftragten

der _____ in _____

In dieser Funktion sind Sie Frau / Herrn OStD _____ unmittelbar unterstellt.

In Zusammenarbeit mit Ihren Kolleginnen und Kollegen obliegt Ihnen die Sicherstellung der Vorschriften zur Wahrung des Persönlichkeitsrechts der Schüler, ihrer Eltern und der hier tätigen Lehrerinnen und Lehrer. Dabei wirken Sie auf die Einhaltung der Vorschriften zum Datenschutz hin durch Beratung der Schulleitung, der Unterrichtenden und der vorgeschriebenen Gremien. Sie überwachen die Umsetzung und Einhaltung von datenschutzrechtlichen Vorgaben und führen gegebenenfalls Mitarbeiterschulungen durch. Zu Ihren Aufgaben gehört auch die Zusammenarbeit mit dem zuständigen Diözesandatenschutzbeauftragten.

In Ihrer Funktion als Datenschutzbeauftragte(r) sind Sie weisungsfrei. Die Schulleitung wird die Ausübung Ihrer Tätigkeit bestmöglich unterstützen und sichert Ihnen zu, dass Sie wegen der Erfüllung dieser Aufgabe nicht benachteiligt werden. Zur Schaffung einer angemessenen Arbeitsgrundlage wird Ihnen eine Übersicht über die Verfahren automatisierter Datenverarbeitung nach § 3a KDO zur Verfügung gestellt. Ihnen wird zudem in angemessenem Umfang Gelegenheit zur eigenen Fortbildung gegeben.

Ich wünsche Ihnen für die Übernahme dieser Aufgabe viel Erfolg und gute Unterstützung.

Mit freundlichen Grüßen

_____	_____
Datum / Ort	Schulleiter/in

– Anlage 4 –

Anlage zu § 6 KDO

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

– Anlage 5 –

Informationen zur pädagogischen Arbeit:

Das klicksafe-Lehrerhandbuch „Knowhow für junge Leser“. Eine praxisnahe Einführung in die weiten Felder der Online- und Netzkommunikationen.

Die klicksafe-Materialien für die Durchführung von Elternabenden. Einbeziehung der Eltern zu wesentlichen Themen der Medienkompetenz.

KlickITsafe – Online Test und Arbeitshefte für die Sekundarstufe I und Grundschulen.

Klicksafe – Broschüren und Ratgeber. Eine Fülle von Schriften für die pädagogische Arbeit zu wichtigen Themen aus den Bereichen Datenschutz – Soziale Netzwerke – Handy – Cybermobbing – Chat – Urheber- und Persönlichkeitsrechte und vielem mehr.

BSI für Bürger. Ins Internet mit Sicherheit. Informationen zu PCs, Internetsicherheit, Mobile Sicherheit, u.a.

Herausgeber:
Der Diözesandatenschutzbeauftragte der (Erz-)Bistümer Berlin, Hamburg, Hildesheim, Magdeburg, Osnabrück und des Bischöflich Münsterschen Offizialats in Vechta i.O.
Engelbosteler Damm 72
30167 Hannover
Tel.: 0511 / 81 93 15
Fax: 0511 / 81 21 35
Internet: http://www.datenschutz-kirche.de

Mail: info@datenschutz-kirche.de
Erscheinungsdatum: Juni 2015