IT-Nutzungsordnung für Schulen

§ 1 Anwendungsbereich, Zielsetzung

(1) Das Bistum Münster erlässt die vorliegende IT-Nutzungsordnung als verbindliche Richtlinie für die Nutzung der IT-Systeme und Anwendungen, insbesondere der Informatikfachräumen (IFR), aller Schulen, die in Trägerschaft des Bistum Münster betrieben werden. Schulen, die sich nicht in Trägerschaft des Bistum Münster befinden, aber durch die Gr. 650 – IT betreut werden (z.B. die Schulen in Trägerschaft der Pfarrgemeinden), wird die Beachtung der vorliegenden Richtlinien zur Gewährleistung eines sicheren IT-Betriebes ebenfalls dringend empfohlen.

(2) Die vorliegende IT-Nutzungsordnung gilt insbesondere für die Nutzung des IFR-Netzes sowie des Gästenetzes, sie gilt nicht für die netzwerkgestützte Schulverwaltung.

(3) Die unterzeichnende Schule verpflichtet sich, die vorliegende IT-Nutzungsordnung vor Nutzung der IT-Systeme und Anwendungen allen beteiligten Nutzern (Lehrer, sonstige Mitarbeiter, Schüler, Gäste etc.) auf geeignete Weise und verbindlich zur Kenntnis zu bringen. Die Nutzung der IT-Systeme und Anwendungen der Schule ist nur unter Einhaltung dieser IT-Nutzungsordnung zulässig. Alternativ kann für reine Endanwender wie z.B. Schüler, Gäste oder Mitarbeiter auch die vereinfachte IT-Benutzerrichtlinie verwendet werden. In Zweifels- und Auslegungsfragen geht die vorliegende IT-Nutzungsordnung der IT-Benutzerrichtlinie vor.

(4) Ziel dieser Nutzungsordnung ist es, die Nutzungsbedingungen sowie die damit verbundenen notwendigen Maßnahmen zur Protokollierung und Kontrolle transparent zu machen, die Persönlichkeitsrechte der Nutzer zu sichern, den Schutz ihrer personenbezogenen Daten zu gewährleisten und Schaden vom Bistum Münster und den Schulen abzuhalten.

§ 2 Allgemeine Verhaltensrichtlinien

(1) Die IT-Systeme und Anwendungen der dienstlichen Schulnetze (Verwaltungsnetz, IFR-Netz) stehen

a. den Lehrern und Mitarbeitern als Arbeitsmittel im Rahmen der dienstlichen Aufgabenerfüllung zur Verfügung, wobei die Nutzung für private Zwecke ausdrücklich untersagt ist
b. den Schülern und Gästen für rein schulische Zwecke zur Verfügung

und dienen insbesondere der Verbesserung der internen und externen Kommunikation, der Erzielung einer höheren Effizienz und der Beschleunigung der Informationsbeschaffung und der Arbeitsprozesse.

(2) Unzulässig ist jede wissentliche oder fahrlässige IT-Nutzung, die geeignet ist, den Interessen oder dem Ansehen des Bistum Münster in der Öffentlichkeit zu schaden, die Sicherheit des Netzwerkes zu beeinträchtigen oder die gegen die geltenden Rechtsvorschriften oder einschlägigen Arbeits- und Sicherheitsanweisungen für die Nutzung der IT-Systeme verstößt. Untersagt ist insbesondere das Abrufen oder Verbreiten von Inhalten, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen, sowie das Abrufen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen.

(3) Das Verbreiten von weltanschaulichen, politischen oder kommerziellen Informationen oder Werbung außerhalb der schulischen oder kirchlichen Zweckbindung über die dienstlichen Netzwerke und Ressourcen ist untersagt.

(4) Mobbing, Nachstellung (Stalking) oder sonstige Belästigungen jeglicher Art gegenüber anderen Schülern, Lehrern oder Personen außerhalb der Schule sind verboten.

(5) Das Abrufen von unmittelbar kostenpflichtigen Informationen oder Dienstleistungen sowie der Abschluss vertraglicher Vereinbarungen im Namen der Schule oder des Bistum Münster ist untersagt (z.B. unmittelbar kostenpflichtige Informationsdienste oder die Kosten verursachende Einwahl über UMTS etc.). Im Rahmen der gestatteten Nutzung dürfen keine kommerziellen oder sonstigen geschäftlichen Zwecke verfolgt werden (z.B. Powerseller bei ebay).

(6) Geräte, Räume, Software und Installationen sowie die gesamte Ausstattung sind pfleglich zu behandeln, nicht zu verschmutzen oder zu beschädigen. Essen, Trinken, Rauchen etc. ist in den Informatikfachräumen (IFR) untersagt. Bei mutwilligen oder leichtfertigen Beschädigungen werden Schadensersatzansprüche erhoben, auf die Haftungsverantwortlichkeit der Erziehungsberechtigten bei Minderjährigen wird hingewiesen.

(7) Die Gr. 650 – IT fungiert als Ansprechstelle, bei der die Nutzer unerlaubte oder rechtswidrige Inhalte, die sie in den IT-Systemen bemerkt haben, bekannt geben sollen, um die Inhalte auf diesem Wege schnellstmöglich zu unterbinden. Jeder Nutzer ist aufgefordert, in dieser Weise der Verbreitung illegaler Inhalte entgegenzuwirken und weiteren Schaden von der Schule und vom Bistum Münster abzuwenden.

§ 3 Hardware, Software, Urheberrecht

(1) Die Nutzer dürfen private Geräte, Hardware oder Software nicht im Rahmen der dienstlichen IT-Systeme verwenden, insbesondere keine private Software installieren. Private oder andere externe Geräte (z.B. Scanner, Drucker, Mobiltelefone, Smartphones, Tablets, Rechner, MP3-Player, Kameras etc.) dürfen nicht an die dienstlichen Schulnetze (Verwaltungsnetz, IFR-Netz) angeschlossen werden. Private Geräte, Hardware oder Software dürfen von den Nutzern aber im Rahmen des Gästenetzes über W-LAN verwendet werden.

(2) Die Installation von Software auf den dienstlichen IT-Systemen darf ausschließlich nur durch Mitarbeiter der Gr. 650 – IT erfolgen. Die Nutzer dürfen im Rahmen der dienstlichen Schulnetze (Verwaltungsnetz, IFR-Netz) ohne Erlaubnis keine fremde Software aus dem Internet herunterladen, wozu auch Bildschirmschoner, Demoprogramme, Computerspiele etc. zu rechnen sind. Ohne besondere Erlaubnis dürfen grundsätzlich keine fremden Programme aus dem Internet oder E-Mail-Anhängen gestartet werden. Es werden spezielle Lehrerprofile angeboten, die eine Nutzung von Online-Applikationen für ausschließlich fachspezifische, schulische Zwecke gestatten. In der Unterrichtssituation können Lehrer die Nutzung der Online-Applikationen ad hoc und zeitlich begrenzt auch für Schüler freischalten. Die Installation oder Nutzung von Spielen jeder Art (z.B. Siedler, CounterStrike, HalfLife), wozu auch Online-Spiele gehören, ist untersagt. Die Verwendung privater Geräte, Hardware oder Software im Rahmen des Gästenetzes über W-LAN ist hiervon nicht betroffen.

(3) Strengstens untersagt ist die Nutzung (Down- und Upload) von File-Sharing-Programmen (P2P-Tauschbörsen), sofern die ordnungsgemäße Lizenzierung nicht schriftlich sichergestellt ist. Ebenso dürfen urheberrechtlich angreifbare oder ausschließlich privat nutzbare MP3-Dateien, Formate, Dateien und Kopien nicht auf dienstlichen Ressourcen vorgehalten werden. Verstöße führen zu hohen Abmahnkosten und Schadensersatzansprüchen seitens externer Rechteinhaber. Die Verursacher werden ermittelt und in Regress genommen, auf die Haftungsverantwortlichkeit der Erziehungsberechtigten bei Minderjährigen wird hingewiesen.

(4) Persönliche Daten der Nutzer (z.B. Dokumente, digitale Fotos etc.) dürfen nur auf dem gesondert eingerichteten „Persönlichen Laufwerk“ des Nutzers gespeichert werden. Die persönlichen Laufwerke der Nutzer unterliegen einer flexiblen Größenbeschränkung, die von der Gr. 650 – IT nach den technischen Erfordernissen festgelegt wird. Eine Speicherung von persönlichen Daten auf dienstlichen IT-Systemen ist grundsätzlich untersagt.

(5) Softwareprodukte, Dokumentationen und Handbücher sind in aller Regel lizenzpflichtig und unterliegen urheberrechtlichen Bestimmungen. Auch (kostenfreie) Freeware, Shareware oder Open Source Software (OSS) ist an lizenzrechtliche Bedingungen gebunden und darf nicht regelfrei eingesetzt werden. Der Einsatz von Freier Software ist, auch wenn sie kostenlos ist, mit der Gr. 650 – IT abzustimmen und nur nach deren Maßgaben zulässig.

(6) Für die Lizenzierung der durch die Gr. 650 – IT bereitgestellten Software ist allein das Bistum Münster verantwortlich. Nachweise über die ordnungsgemäße Lizenzierung können durch das Bistum Münster jederzeit zur Verfügung gestellt werden. Für jede weitere Software, die durch die Schule verwendet wird, ist die ordnungsgemäße Lizenzierung durch die Schule schriftlich nachzuweisen, was auch für jede Art von Freier Software gilt. Die zur Verfügung gestellte Software darf grundsätzlich nur für dienstliche Zwecke verwendet werden, die Nutzung für private Zwecke ist untersagt.

(7) Ausnahmen zu den voranstehenden Regelungen sind nur mit vorheriger schriftlicher Zustimmung der Gr. 650 – IT möglich.

§ 4 Server und zentrale Ressourcen

(1) Die Installation von Software auf den Servern ist für Nutzer und Schulen untersagt, Ausnahmen müssen durch die Gr. 650 - IT schriftlich genehmigt werden. Die technische Konfiguration der Server oder der IT-Infrastruktur (Hard- und Software, Einstellungen) darf nicht verändert werden.

(2) Grundsätzlich sind die Räume in den Schulen, in denen sich die Server befinden, ständig verschlossen zu halten. Der Zutritt gemäß IV. Anlage zu § 6 Nr. 1 KDO-DVO ist nur Lehrern oder autorisierten Personen zu gewähren. Wird der Serverraum auch anderweitig genutzt, ist dafür zu sorgen, dass die Serverschränke verschlossen werden und gegen Fremdmanipulationen geschützt sind.

(3) Andere Geräte der zentralen IT-Infrastruktur, z.B. Switches, Repeater, Internetanschluss, Verkabelung etc. sind entsprechend zu sichern.

§ 5 Technische Sicherungssysteme

(1) Die Gr. 650 – IT ist für die Sicherheit der IT-Systeme sowie den nachfolgenden Einsatz von Sicherungssystemen und Sicherungsmaßnahmen ausschließlich zuständig und verantwortlich. Weitere Einzelheiten sind den jeweiligen Dokumentationen, Sicherheitsrichtlinien bzw. Herstellerhinweisen zu entnehmen.

(2) Viren- und Spywarefilter: Dieser löscht insbesondere virenbehaftete Dateien automatisch oder stellt sie in Quarantäne. Der betroffene Nutzer wird über eine eventuelle Löschung nicht benachrichtigt. Alle Datenbestände, die von extern stammen (z.B. USB-Stick, CD, DVD), müssen von den Nutzern durch eine aktuelle Virenschutzsoftware des Bistum Münster gesondert überprüft werden. Die Gr. 650 – IT stellt entsprechende technische Funktionalitäten zur Verfügung. Viren, Trojaner oder andere Schadsoftware dürfen von den Nutzern nicht verbreitet oder vorgehalten werden.

(3) URL-Filter: Unzulässige oder strafbare Webseiten oder Kategorien werden für den Zugriff gesperrt. Bei Aufruf gesperrter Seiten erhält der Nutzer eine Hinweismeldung über die Sperrung. In der Regel werden alle Nutzer gleich behandelt. Bei besonderen Anforderungen oder auf individuelle Anfragen, die sich aus der Aufgabenstellung der Nutzer ergeben, können gesperrte Seiten durch die Gr. 650 – IT freigeschaltet werden.

(4) Firewall: Unzulässige Zugriffe von außen werden durch den Einsatz einer Firewall sowie einem Intrusion Detection System (IDS) unterbunden. Es erfolgt eine entsprechende Protokollierung der Aktivitäten.

(5) Einbruchsversuche (Hacking) oder unberechtigte Zugriffsversuche jeder Art, jegliche Veränderung der Installationen oder Konfigurationen auf Rechnern oder Servern sowie die Entfernung oder Umgehung von Sicherheitsmaßnahmen sind strikt untersagt.

(6) Verschlüsselungspflicht: Die Verwendung externer Datenträger (z.B. USB-Stick, CD, DVD) für personenbezogene Daten aus dem Schulbetrieb ist gemäß § 6 KDO, IV. Anlage zu § 6 KDO Nr. 2 und 4 KDO-DVO, § 3 KDO-Schulen nur zulässig, wenn die externen Datenträger ausreichend sicher verschlüsselt werden. Die Gr. 650 – IT stellt eine entsprechende technische Verschlüsselungslösung zur Verfügung.

(7) Die Nutzer sind zum vertraulichen Umgang mit Benutzernamen, Passwörtern oder sonstigen Zugangsberechtigungen verpflichtet. Insbesondere dürfen die Zugangsinformationen nicht weitergegeben, ungesichert vorgehalten oder transportiert werden. Die Nutzung über Benutzername / Kennwort wird mit der eigenen, persönlichen Nutzung gleichgesetzt. Nutzt ein Dritter ein persönliches Kennwort, so kann der Kennwortinhaberin Zurechnungsschwierigkeiten geraten.

(8) Die Nutzer dürfen nicht auf Netzwerkbereiche oder Datenträger zugreifen, die für sie oder ihr Aufgabengebiet nicht freigegeben oder vorgesehen sind. Die offiziell vergebenen Zugriffsrechte dürfen durch die Nutzer nicht eigenständig erweitert werden. Dies gilt auch dann, wenn durch unzureichende Rechtevergabe oder technische Mängel ein Zugriff tatsächlich möglich oder angezeigt wäre. Das eigene Verzeichnis darf anderen Nutzern nicht zugänglich gemacht werden (z.B. durch Freigabe oder Weitergabe des Passworts).

(9) Die Administratoren des Bistums Münster, Gr. 650 – IT, sind ausschließlich verantwortlich für die Installation, Betreuung und einwandfreie Funktion aller IT-Komponenten. Der eigenständige Betrieb von Netzwerken oder Internetzugängen durch die Schulen außerhalb der von der Gr. 650 – IT zur Verfügung gestellten Ressourcen ist aus sicherheitstechnischen Gründen untersagt.

§ 6 Datensicherung

Zum Zwecke der Datensicherung wird gemäß § 6 KDO, IV. Anlage zu § 6 KDO Nr. 7 KDO-DVO gestuft nach Generationen ein Backup-System betrieben, mit dessen Hilfe im Notfall alle relevanten Daten wieder hergestellt werden können. Die Backup-Dateien werden nach spätestens zwei Jahren zum Jahresende gelöscht.

§ 7 Protokollierung

(1) Auf den hierzu vorgesehenen Systemen (Proxy-Server etc.) und Filtereinrichtungen (Firewall, URL-Filter etc.) können Nutzungsdaten (etwa der E-Mail und Internet-Nutzung), insbesondere mit Angaben

- von Datum und Uhrzeit
- der Dauer der Datenübertragung
- des eingehenden und ausgehenden Datenvolumens,
- der Adressen von Absendern und Empfängern
- der Adresse der Internetseiten
- der Client-Nummer, Adresse des Zielrechners
- der E-Mail-ID

- der Art des in Anspruch genommenen Dienstes (z.B. Zugriff auf Internetseite, E-Mail, Datentransfer, Zugriff auf externe Rechner etc.)

protokolliert werden. Dies ist aus Datensicherheitsgründen und für eine Störungsbeseitigung erforderlich. Aus den Protokollen gehen die Aktivitäten der Nutzer hervor.

(2) Die Protokolldateien unterliegen der Zweckbindung dieser Nutzungsordnung und werden automatisiert nach einer Frist von spätestens 3 Monaten wieder gelöscht.

§ 8 Auswertung und Kontrolle

(1) Die aufgezeichneten Protokolldateien, andere Daten oder Dateien können statistisch (ohne Personenbezug) durch manuelle Stichproben oder automatisiert ausgewertet werden. Der Datenschutzbeauftragte wird auf Wunsch an den Auswertungen beteiligt.

(2) Das Bistum Münster schafft die Voraussetzungen für ein gestuftes Kontrollverfahren, insbesondere durch Installation von Funktionen, die eine anonyme Auswertung ebenso wie die Repersonalisierung der Daten ermöglichen. Es ist technisch oder organisatorisch sicherzustellen, dass bei der anonymen Auswertung keine personenbezogenen Daten eingesehen werden können.

(3) Im Rahmen von administrativen Aufgaben oder Wartungsarbeiten der Gr. 650 – IT kann ein Zugriff auf dienstliche Daten, Dateien, Dienste oder Verzeichnisse erforderlich werden. Um die Arbeiten der Gr. 650 – IT nicht zu behindern, dürfen die bestehenden Zugriffsrechte auf die Inhalte des persönlichen Laufwerks durch den Nutzer nicht verändert oder eingeschränkt werden (z.B. über Dateisystemrechte etc.).

(4) Ergibt sich aufgrund der anonymen Auswertung, einer Meldung oder anderer Verdachtsmomente ein konkreter Verdacht auf eine strafbare oder missbräuchliche Nutzung, erfolgt nach vorheriger Absprache mit dem Datenschutzbeauftragten eine personenbezogene Überprüfung des Vorgangs. Die tatsächlichen Anhaltspunkte, welche den konkreten Verdacht begründen, sind zu dokumentieren. Eine personenbezogene Überprüfung ist auf gravierende Missbrauchsfälle beschränkt, Bagatellfälle rechtfertigen die personenbezogene Überprüfung nicht. Ein Kontrollzugriff auf das persönliche Laufwerk des Nutzers ist nur in besonders schwerwiegenden Fällen zulässig.

(5) Bestätigt die Überprüfung den Verdacht, so wird ein gemeinsamer Bericht erstellt und der betroffene Nutzer angehört. Wird der Verdacht durch die Überprüfung nicht bestätigt, so sind die für die Überprüfung erhobenen Daten und Aufzeichnungen unverzüglich zu löschen. Die nicht bestätigte Überprüfung darf keinerlei weitere Folgemaßnahmen – insbesondere keine gezielten Stichproben - nach sich ziehen. Fehlt bei gravierenden Verdachtsmomenten auf eine Straftat die Nachweismöglichkeit, so können die Ermittlungsbehörden eingeschaltet werden.

(6) Bei Gefahr im Verzug können bedrohliche Situationen oder strafbare Handlungen unmittelbar unterbunden werden, insbesondere werden die erforderlichen technischen Abwehrmaßnahmen ohne Verzögerung ergriffen, auch wenn hierbei personenbezogene Daten eingesehen werden müssen. Der Datenschutzbeauftragte ist sobald wie möglich über die Vorgänge zu informieren.

(7) Trotz der voranstehenden Regelungen bleibt die Schulleitung dafür verantwortlich, altersgerechte Kontroll- und Aufsichtsmaßnahmen durch das Lehrpersonal umzusetzen, da auch Kinder und Jugendliche einen Internetzugang erhalten.

§ 9 Veröffentlichung, Einwilligung

(1) Bilder, Videoaufnahmen, Dokumente etc. aus dem Schulbereich (z.B. Lehrer, Mitschüler, Gebäude) dürfen aus lizenz- und datenschutzrechtlichen Gründen nur mit Einwilligung der Betroffenen und der Schulleitung im Internet (z.B. Facebook, Youtube) oder Intranet (z.B. Schüler-Lehrer-Plattform) veröffentlicht werden. Das Recht am eigenen Bild ist zu beachten.

(2) Schulleitung und Lehrer sind verpflichtet, die notwendigen datenschutzrechtlichen Einwilligungen der Betroffenen für die Veröffentlichung von Daten und Bildern einzuholen. Bei Minderjährigen ist die Einwilligung der Erziehungsberechtigten erforderlich, bei Jugendlichen ab 16 Jahren zusätzlich auch deren eigene Einwilligung. Einwilligungen sind in der Regel schriftlich einzuholen.

(3) Die Schulen sind gehalten, den persönlichen Zugang zu Internet und Netzwerken für Kinder und Jugendliche nur nach vorheriger schriftlicher Einwilligung der Erziehungsberechtigten zu gewähren. Ein entsprechendes Formular sollte bereits bei der Einschulung verwendet werden. Die Möglichkeit der Verwendung des Internets in der Unterrichtssituation bleibt davon unberührt.

§ 10 Zweckbindung und Datengeheimnis

(1) Die im Rahmen der vorliegenden Nutzungsordnung anfallenden personenbezogenen Daten (Protokolldateien, Auswertungsergebnisse, Wartungszugriffe etc.) werden ausschließlich zu Zwecken der Analyse und Korrektur technischer Fehler, Gewährleistung der Systemsicherheit, Optimierung des Netzes, statistischen Feststellungen, bei Gefahr im Verzug, Störungen, Angriffen auf das Netz und Verdacht auf eine Straftat sowie für Auswertungen gemäß dieser Nutzungsordnung verwendet.

(2) Im übrigen werden die anfallenden personenbezogenen Daten nicht zur Leistungs- und Verhaltenskontrolle verwendet.

(3) Die mit der Verwendung personenbezogener Daten betrauten Personen sind gemäß § 4 KDO durch eine schriftliche, unterschriebene Erklärung auf die Einhaltung der Datenschutzbestimmungen zu verpflichten und auf die strafrechtlichen, arbeitsrechtlichen und zivilrechtlichen Konsequenzen bei Verstößen hinzuweisen. Die mit Administrations-, Auswertungs- und Kontrollmaßnahmen betrauten Personen werden in besonderem Maße auf ihre Verantwortung und das Datengeheimnis gemäß § 4 KDO verpflichtet. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 11 Haftung

(1) Die gewährte Nutzungsmöglichkeit ist eine unverbindliche, jederzeit widerrufbare Vergünstigung, auf die kein Anspruch besteht. Dienstliche Belange haben stets Vorrang. Sofern aus dienstlichen Gründen erforderlich, kann die sonstige Nutzung zeitweise unterbunden werden.

(2) Die Schule bzw. das Bistum Münster übernehmen keine Gewähr für die Verfügbarkeit der Nutzung. Die Haftung des Bistum Münster gegenüber den Nutzern im Zusammenhang mit der kostenfrei gewährten Nutzungsmöglichkeit ist ausgeschlossen, soweit nicht Vorsatz oder grobe Fahrlässigkeit des Bistum Münster nach § 521 BGB vorliegen.

§ 12 Konsequenzen bei Verstößen

(1) Bei Zuwiderhandlung gegen diese Nutzungsordnung oder unsachgemäßer Nutzung können zur Wahrung der Sicherheit die Internet- oder Netzwerk-Zugänge deaktiviert werden. Die Schule ist daher verpflichtet, die systemrelevanten Abteilungen des Trägers (650 - IT und 330 - Katholische Schulen) umgehend einzubeziehen.

(2) Bei gravierenden Verstößen verpflichtet sich die Schule, in enger Zusammenarbeit mit dem Träger, mit angemessenen Maßnahmen zu reagieren, dies umfasst insbesondere

- Entzug der Nutzungsberechtigung
- schulrechtliche Ordnungsmaßnahmen
- arbeitsrechtliche Konsequenzen bis hin zur Kündigung des Arbeitsverhältnisses
- zivilrechtliche Schritte, insbesondere Schadensersatzansprüche bei mutwilliger oder leichtfertiger Schadensverursachung auch gegen die Erziehungsberechtigten
- Strafanzeige

(3) Erhebt das Bistum Münster personenbezogene Daten unter Verstoß gegen die Vorgaben dieser Nutzungsordnung, so unterfallen die Daten einem Beweisverwertungsverbot mit der Folge, dass sie für Sanktionen nicht verwendet werden können.

§ 13 Übergangsregelung

(1) Ergänzend zu § 3 Abs. 2 und § 5 Abs. 9 IT-Nutzungsordnung gilt diese Übergangsregelung bis zur vollständigen Umsetzung des Medienentwicklungsplans (MEP). Anschließend tritt sie selbstständig wieder außer Kraft.

(2) Unter den nachfolgenden Bedingungen darf eine eigenverantwortliche Installation von Software durch die Schulen auch ohne Mitwirkung der Gr. 650 – IT erfolgen.

a. Die Installation darf nur auf von den Schulen eigenverwalteten Systemen (Rechnern) erfolgen. Nach vollständiger Umsetzung des MEP entfallen die eigenverwalteten Systeme (Rechner).
b. Installiert werden dürfen nur fachspezifische, für schulische Zwecke erforderliche Programme.

(3) Die Administratoren der Schulen sind für die Installation, Betreuung und fehlerfreie Funktion der eigenverwalteten Systeme (Rechner, Software etc.) selbst verantwortlich.

(4) Die rechtliche, insbesondere urheberrechtliche, und IT-sicherheitstechnische Verantwortlichkeit für die eigenverwalteten Systeme (Rechner, Software etc.) liegt bei den Schulleitungen.

§ 14 Schlussbestimmungen

(1) Die gemäß § 13a KDO erforderliche Benachrichtigung über die Speicherung personenbezogener Daten nach dieser Nutzungsordnung erfolgt gemäß § 13a Abs. 2 Nr. 1 KDO durch Bekanntgabe der Nutzungsordnung gegenüber den betroffenen Nutzern. Die Schulen sind zur Bekanntgabe der Nutzungsordnung gegenüber den Nutzern in geeigneter Weise über die gewohnten Informationskanäle (z.B. Aushang in der Schule, Rundmail etc.) verpflichtet.

(2) Geplante Änderungen oder Erweiterungen der IT-Systeme oder Anwendungen werden dem Datenschutzbeauftragten rechtzeitig mitgeteilt, soweit sie sich auf die Regelungen dieser Nutzungsordnung auswirken. Notwendige Änderungen oder Erweiterungen dieser Nutzungsordnung können in einer ergänzenden Regelung vorgenommen werden.

(3) Diese Nutzungsordnung tritt mit Unterzeichnung durch das Bistum Münster und Bekanntgabe in den Schulen in Kraft. Die datenschutzrechtlichen Regelungen, insbesondere der KDO, KDO-DVO und KDO-Schulen bleiben unberührt und gelten ergänzend.