# IT- Benutzerrichtlinie für Schulen



## § 1 Anwendungsbereich, Zielsetzung

(1) Die vorliegende IT-Benutzerrichtlinie regelt verbindlich die Nutzung der IT-Systeme und Anwendungen, insbesondere der Informatikfachräumen (IFR), aller Schulen des Bistum Münster. Sie gilt für die Nutzung des IFR-Netzes sowie des Gästenetzes.

(2) Die IT-Benutzerrichtlinie will die Nutzungsbedingungen sowie die damit verbundenen notwendigen Maßnahmen zur Protokollierung und Kontrolle transparent machen, die Persönlichkeitsrechte der Nutzer schützen und Schaden vom Bistum Münster und den Schulen abhalten.

## § 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.

(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) Bei der Gr. 650 – IT können unerlaubte oder rechtswidrige Inhalte, die in den IT-Systemen bemerkt werden, gemeldet werden, 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 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. 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) 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 Technische Sicherungssysteme

(1) 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.

(2) 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.

(3) 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.

(4) Verschlüsselungspflicht: Die Verwendung externer Datenträger (z.B. USB-Stick, CD, DVD) für personenbezogene Daten aus dem Schulbetrieb ist nach den gesetzlichen Vorgaben nur zulässig, wenn die externen Datenträger ausreichend sicher verschlüsselt werden. Die Gr. 650 – IT stellt eine entsprechende technische Verschlüsselungslösung zur Verfügung.

(5) 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.

(6) 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).

## § 5 Protokollierung

(1) Auf den hierzu vorgesehenen IT-Systemen können Nutzungsdaten (etwa der E-Mail und Internet-Nutzung) 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.

## § 6 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) 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.

(4) 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.

### § 7 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.

## § 8 Konsequenzen bei Verstößen

(1) Bei gravierenden Verstößen gegen die vorliegende IT-Benutzerrichtlinie ist die Schule verpflichtet, 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

(2) 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.

## § 9 Schlussbestimmungen

(1) Die vorliegende IT-Benutzerrichtlinie tritt zusammen mit Unterzeichnung der zugehörigen IT-Nutzungsordnung durch das Bistum Münster und Bekanntgabe in den Schulen in Kraft.

(2) Die vorliegende IT-Benutzerrichtlinie dient der einfacheren Darstellung der IT-Nutzungsbedingungen für den Endanwender. In Zweifels- und Auslegungsfragen geht die detaillierte IT-Nutzungsordnung der vorliegenden IT-Benutzerrichtlinie vor.

Münster, den …..

_____

Kenntnisnahmebestätigung Nutzer