Merkblatt
für die Nutzung von IT-Systemen

(Stand 01.09.2012)

Die Daten im Jugendhilfezentrum Marl unterliegen einer besonderen Schutzwürdigkeit. Innerhalb der Einrichtungen werden Daten verarbeitet, die für das berufliche und private Umfeld der Bewohner und Bewohnerinnen wie auch der Beschäftigten von höchster Bedeutung sind. Die Entwicklungen auf dem Gebiet der Informationstechnologie bieten neue Möglichkeiten, aber auch neue Gefahren.

Durch die „Dienstanweisung für die Nutzung von IT-Systemen“ sollen mögliche Gefährdungspotentiale verringert werden, indem Bestimmungen des Datenschutzes, Anforderungen an die Sicherheit sowie die Erfordernisse des Dienstbetriebes geregelt werden. Rechtsvorschriften über den Datenschutz bleiben hiervon unberührt. Unter IT-Systeme sind dabei insbesondere Arbeitsplatzrechner, zentrale Rechner (z.B. Server), Datenendgräte (z.B. Drucker oder Scanner) einschließlich der genutzten Programme zu verstehen.

Wir bitten Sie daher, in Ihrer täglichen Arbeit die nachfolgenden Regelungen zu beachten.

Zugangsberechtigung

(1) Beim Verlassen des Arbeitsplatzes hat der Benutzer bzw. Benutzerin das System abzumelden bzw. für den Zugang durch unbefugte Dritte zu sperren. Danach darf der Zugriff auf Datenbestände nur durch die erneute Eingabe des Passwortes möglich sein.

(2) Es muss dafür gesorgt werden, dass bei Darstellung von personenbezogenen Daten auf Bildschirmen und Druckern Unbefugten die Einsicht verwehrt wird.

(3) Das Betreten von Räumen, in denen sich IT-Systeme befinden, ist nur Bediensteten gestattet. Dritte dürfen die Räume unter Beachtung von (2) nur bei Anwesenheit von Bediensteten betreten. Zu den Dritten zählt u. a. auch der Wartungsdienst.

Zugriffsberechtigung

(1) IT-Systeme dürfen nur von den Bediensteten genutzt werden, die hierzu ermächtigt worden sind.

(2) Benutzer und Benutzerinnen dürfen nur auf Daten und Programme zugreifen, die sie im Rahmen der ihnen übertragenen Aufgaben benötigen. Die Zugriffsrechte werden von der LWL.IT Service Abteilung eingerichtet, geändert, verwaltet und gelöscht. Hier wird auch eine aktuelle Übersicht über die vergebenen Berechtigungen schriftlich geführt.

(3) Beim Speichern von Daten ist darauf zu achten, dass personenbezogene Daten nur in Verzeichnisse von zugriffsberechtigten Personen abgelegt werden.

(4) Bei der Verwendung von externen Daten sind die zu übernehmenden Daten auf mögliche Gefährdungen des Systems zu überprüfen. Insbesondere sind die zu übernehmenden Daten mit einem aktuellen Virenscanner zu überprüfen

(5) Eine Übermittlung von personenbezogenen Daten darf nur erfolgen soweit dies rechtlich zulässig ist.

Anschrift: Rappaportstraße 8b, 45768 Marl
Telefon: 02365 92488-0
Telefax: 02365 92488-133
E-Mail: jhz.mail@lwl.org
Internet: www.lwl-jugendhilfezentrum.de

Bankverbindung:
Sparkasse Vest Recklinghausen
Kto-Nr.: 650 059 10, BLZ: 426 501 50
IBAN: DE19 4265 0150 0065 0059 10
BIC: WELADED1REK

Arbeitsstation

(1) Die Deinstallation einzelner Komponenten, die Installation von Programmen wie auch Eingriffe in die Hardware-Konfiguration werden nur von der LWL.IT Service Abteilung vorgenommen.

(2) Bei vernetzten Systemen sind Daten grundsätzlich auf zentralen Laufwerken zu speichern. Datenbestände auf der lokalen Festplatte (Laufwerk C:) werden nicht gesichert.

(3) Änderungen an den installierten IT-Systemen (z.B. Austausch von Hardwareteilen, Installation oder Deinstallation von Programmen) sind nur in Abstimmung mit der LWL.IT Service Abteilung zulässig. Dies gilt auch für den Austausch oder der Wartung von Hardwareteilen sowie für den Standortwechsel.

(4) Der Anschluss eines mobilen Rechners (z.B. Laptop, Palmtop) an das lokale Netz oder an die vernetzten Arbeitsplatzrechner darf nur nach den von der LWL.IT Service Abteilung festgelegten Vorgehensweise erfolgen.

(5) Eine Speicherung von personenbezogenen Daten auf mobilen Rechner sollte nicht erfolgen. Falls dies dennoch erforderlich ist, sind die personenbezogenen Daten zu verschlüsseln.

(6) Ansonsten wird auf die „Dienstanweisung zum Datenschutz“ verwiesen.

Passwort

(1) Passworte dürfen nicht aus einer zu einfachen Ziffern- und / oder Buchstabenkombination, aus einfach abzuleitenden Begriffen oder leicht zu erratenden Namen (z.B. Name von Angehörigen, Monatsname) bestehen. Es sollte möglichst eine Kombination aus Buchstaben und Ziffern ohne erkennbare Gesetzesmäßigkeit verwendet werden.

(2) Passworte sollten mindestens 8-stellig sein. Sollten die IT-Systeme diese Mindestlänge nicht unterstützen, ist die maximal mögliche Anzahl zu verwenden.

(3) Die Zahl der erlaubten Passwort-Fehlversuche sollte auf 3 beschränkt sein.

(4) Benutzer und Benutzerinnen haben darüber hinaus folgendes zu beachten:
- Passworte dürfen nur dann eingegeben werden, wenn die Eingabe nicht von Unbefugten beobachtet werden kann.
- Die Passworte sind geheim zu halten.

- Um die Vertraulichkeit der Passworte zu gewährleisten, sind sie spätestens nach Ablauf der von der Systemadministration festzulegenden Gültigkeitsintervalle zu ändern. Die Gültigkeitsintervalle sollten drei Monate nicht überschreiten.

- Sind Passworte Unbefugten bekannt geworden oder besteht ein entsprechender Verdacht, hat die Benutzerin oder der Benutzer unverzüglich das Passwort zu ändern oder eine Änderung zu veranlassen, falls sie selbst nicht änderungsberechtigt ist.

- Passworte sollten nach Möglichkeit nicht aufgeschrieben werden. Falls dies dennoch geschieht, ist dafür Sorge zu tragen, dass keine andere Person die Möglichkeit erhält, diese Aufzeichnung einzusehen.

(5) Detailliertere Informationen entnehmen Sie bitte der Anweisung „Umgang mit Passworten an TUIV-Arbeitsplätzen“

Datenträger

(1) Datenträger mit personenbezogenen Daten oder Programmen dürfen nur in den für sie bestimmten Räumen aufbewahrt und nur von Berechtigten befördert und genutzt werden.

(2) Das Kopieren von Datenträgern wird nur von der Systemadministration zur Datensicherung und zur Fehleranalyse, von den Anwendern zur Sicherung der Anwendungsdaten unter ihrer Benutzerkennung im Rahmen dienstlich vorgeschriebener Sicherungsverfahren oder bei Anordnung im Einzelfall durchgeführt.

(3) Für den Datenaustausch und die Datensicherung dürfen nur die von der LWL.IT Service Abteilung oder von autorisierten Stellen übergebenen Datenträger bzw. Magnetbänder verwendet werden.

(4) Datenträger dürfen erst nach Überprüfung auf Virenbefall eingespielt werden.

(5) Nicht benötigte Datenträger mit personenbezogenen Daten sind unter Verschluss zu halten, oder ordnungsgemäß zu vernichten.

Vorkommnisse

Melden Sie unerklärliche Vorkommnisse (z.B. Fehlermeldungen, Datenverluste, etc.) sofort ihrer LWL.IT Service Abteilung (*1111).

Ansprechpartner für Datenschutz

Für Fragen des Datenschutzes stehen Ihnen folgende Ansprechpartner/innen zur Verfügung:

LWL-Ansprechpartner für Datenschutz:
Datenschutzbeauftragter
Robert Büscher
Tel.: 0251 591-3336
Fax: 0251 591-713336
E-Mail: robert.buescher@lwl.org

Allgemeine Informationen zum Datenschutz im LWL:
http://intranet.itz.lwl.org/de/LWL/Anbieter/LWL-Haupt_und_Personalabteilung/referat-12/Datenschutz/

Michael Baune Betriebsleiter	Werner Kroll Pädagogischer Leiter	Ivo Schweda Verwaltungsleiter

LWL
Für die Menschen.
Für Westfalen-Lippe.

Merkblatt
für die Nutzung von Internet-Diensten
(Stand: 01.09.2012)

Folgende Internet-Dienste sind im Netz des LWL verfügbar:

- WWW (World Wide Web)
- FTP (File Transfer Protocol)
- E-Mail

Zur Nutzung von Internet-Diensten gelten folgende Regelungen:

Die Nutzung von Internet-Diensten ist nur für dienstliche Zwecke zugelassen.

(1) Die Nutzung für außerdienstliche Zwecke wie beispielsweise Internetshopping für den privaten Einkauf oder das Versenden privater E-Mails ist nicht gestattet.

(2) Insbesondere ist abgesehen von dienstlich begründeten Erfordernissen, die vorab anzumelden sind,

- das Abrufen, Anbieten oder Verbreiten von rechtswidrigen Inhalten, insbesondere solchen, die gegen strafrechtliche, datenschutzrechtliche, persönlichkeits-, rechtliche, lizenz- oder urheberrechtliche Bestimmungen verstoßen,
- das Abrufen, Anbieten und Verbreiten von politischen, diskriminierenden, diffamierenden oder verfassungsfeindlichen Informationen (z.B. rassistischer, sexistischer oder pornografischer Art) und das Herunterladen von Spielen

nicht erlaubt.

Der Datenverkehr vom und zum Internet wird von einem Firewall-System aufgezeichnet.

(1) Für jede aufgebaute Verbindung werden Datum, Uhrzeit, Quelle, Ziel und Dienst protokolliert.

(2) Protokolldateien werden in der DV-Zentrale des LWL 1 Jahr vorgehalten und anschließend gelöscht.

(3) Sollen Protokolle zur Feststellung einer Dienstpflichtverletzung ausgewertet werden, informiert die Betriebsleitung vorab den Vorsitzenden / die Vorsitzende des örtlichen Personalrates.

Besondere Regelungen für das E-Mailing.

(1) Jeder Mitarbeiter / jede Mitarbeiterin, die über einen APC-Büroarbeitsplatz verfügt, erhält eine E-Mail-Adresse.

(2) Das Bürokommunikationsprogramm Outlook sollte stets geöffnet sein, damit der Empfang eingehender Nachrichten sofort angezeigt wird. Ansonsten ist mindestens einmal pro Arbeitstag der E-Mail-Eingang zu überprüfen.

(3) Der Versand von E-Mails erfolgt systembedingt grundsätzlich unverschlüsselt. Ein unberechtigter Zugriff auf diese Daten bzw. eine Manipulation kann somit nicht ausgeschlossen werden. Es ist deshalb unzulässig, Daten per E-Mail unverschlüsselt zu übermitteln, für die ein unberechtigter Zugriff oder eine Manipulation ausgeschlossen werden muss. Dies gilt insbesondere für personenbezogene oder personenbeziehbare Daten sowie andere vertrauliche Informationen und Geschäftsgeheimnisse.

(4) Die per E-Mail übermittelten Informationen sind derzeit noch nicht rechtsverbindlich. Folglich dürfen auf diesem Weg z. B. keine Verträge geschlossen bzw. gekündigt oder andere Rechtsgeschäfte abgeschlossen werden (fehlende Beweiskraft im Streitfall).

(5) Der Absender einer E-Mail wird über die erfolgreiche Zustellung systemseitig nicht informiert. Wollen Sie sicher sein, dass Ihre Mail angekommen ist, bitten Sie den Empfänger, / die Empfängerin eine Eingangsbestätigung als Quittung zurückzusenden.

(6) Einer E-Mail kann eine Anlage beigefügt werden.

Vorsicht, Anlagen können Computer-Viren enthalten.

Eingehende E-Mails werden automatisiert zentral auf Viren hin überprüft. Dennoch ist es nicht absolut sichergestellt, dass jeder Virus identifiziert wird. Öffnen Sie deshalb keine Anlagen von E-Mails, die Ihnen von Unbekannten unaufgefordert zugesandt werden. In Zweifelsfällen wenden Sie sich bitte an die EDV-Hotline *1111.

(7) Ansonsten wird auf die „Besondere Geschäftsanweisung zum Umgang mit E-Mails beim LWL“ vom 15.10.2007 verwiesen siehe BGA - E-Mail

Michael Baune Betriebsleiter	Werner Kroll Pädagogischer Leiter	Ivo Schweda Verwaltungsleiter

LWL
Für die Menschen.
Für Westfalen-Lippe.

Merkblatt
Verhalten im Brandfall

BRÄNDE VERHÜTEN

- Offene Flammen - Kerzen etc. - vermeiden
- Defekte Geräte vom Netz trennen; Reparatur veranlassen
- Keine unnötigen Brandlasten in Arbeitsbereichen ansammeln
- Rettungswege und Notausgänge unbedingt frei halten

BRAND MELDEN

- Druckknopfmelder betätigen, wenn vorhanden
- Feuerwehr über Notruf 0-112 (112) alarmieren

IN SICHERHEIT BRINGEN

- Gefährdete / behinderte Personen und Kinder mitnehmen
- Auf Vollzähligkeit achten
- Auf Fluchtwegbeschilderung achten
- Türen / Brandschutztüren schließen
- Keinen Aufzug benutzen
- Auf den Stationen/Gruppen: entweder horizontale Evakuierung auf einer Etage, die Türen auf der B/D-Seite zwischen den Stationen/Gruppen sind Brandschutztüren und halten 30 Minuten einem Feuer stand oder Flucht nach draußen: Sammelpunkt am Festsaal

BRAND BEKÄMPFEN

- Sich dabei selbst nicht gefährden!
- Brandherd mit Löschdecke (sofern vorhanden) vollständig abdecken
- Feuerlöscher (in den Gruppen/Teams vorhanden) erst am Brandherd in Betrieb nehmen
- Ggf. Wasser verwenden (Hydranten, Eimer usw.)
- Kein Wasser bei Fett- und Elektrobränden!
- Feuerlöscher nach Entsicherung warten lassen!

Die Betriebsleitung
Der Brandschutzbeauftragte