IT-Kodex

Beschlossen vom Stadtrat am 28. Juni 2004

1. Einleitung

1.1 Zweck des IT-Kodex

Für die Verarbeitung der ständig wachsenden Menge von Verwaltungsdaten stellt Ihnen die Stadt moderne Anwendungen der Informationstechnologie (IT) zur Verfügung. Die Verwaltungsdaten und die IT-Lösungen für deren Verarbeitung (z.B. Computer, Programme und Netzwerke) bilden einen wesentlichen Wertbestand der Stadt. Durch ihr korrektes, verantwortungsvolles und sorgfältiges Verhalten leisten Sie einen wesentlichen Beitrag zum Schutz der IT-Lösungen der Stadt und der damit verwalteten Daten.

1.2 Stellenwert des IT-Kodex

Der IT-Kodex hat den Status einer verbindlichen Weisung und ist integrierender Bestandteil des Arbeitsvertrages

1.3 Geltungsbereich

Der IT-Kodex gilt für alle Angestellten und Lehrpersonen der Stadt. im Verhältnis zu Aussenstehenden, welche in Berührung mit der städtischen IT gelangen (z.B. Dienstleister, welche mit der städtischen Informatik oder städtischen Daten arbeiten) ist der IT-Kodex in einer entsprechenden Vereinbarung als anwendbar zu erklären.

1.4 Unterstützung

Wenn Sie in der Handhabung des IT-Kodex unsicher sind, oder wenn Sie Fragen im Zusammenhang mit den IT-Anwendungen haben, sind Sie verpflichtet, das IT-Supportcenter der Stadt um Hilfe anzufragen. Nutzen Sie im Intranet der Stadt die Anwendung „IT-Supportcenter“ und eröffnen Sie eine entsprechende Anfrage.

1.5 Verstösse

[1] Verstösse gegen den IT-Kodex gefährden einen wesentlichen Werbestand der Stadt und können schwerwiegende Folgen haben für das Funktionieren der Stadtverwaltung.

[2] Verstösse können personalrechtliche Konsequenzen bis hin zur Auflösung des Arbeitsverhältnisses nach sich ziehen. Schwerwiegende Verstösse (z.B. durch Verletzung des Urheberrechts, des Persönlichkeitsrechts, des Datenschutzes oder die Preisgabe von Dienstgeheimnissen) können für den/die Verantwortliche/n zudem zivil- und/oder strafrechtliche Folgen haben.

1.6 Kontrolle

[1] Zu technischen Zwecken erstellt das Amt für Telematik Statistiken über die Nutzung der IT-Lösungen als Planungsgrundlage für den technischen Betrieb (z.B. Statistik über die Netzwerkauslastung, Speicherbelegung etc.).

[2] Bei begründetem Verdacht auf Missbrauch kann das Amt für Telematik weitergehende Kontrollen über die Benutzung der IT-Lösungen der Stadt anordnen. Es orientiert darüber den Stadtschreiber und dieser den zuständigen Departementsvorsteher. Die gesetzlichen Vorschriften bezüglich Daten- und Persönlichkeitsschutz werden dabei eingehalten.

2. Umgang mit Verwaltungsdaten

2.1 Grundsätzliches

Der Umgang mit Verwaltungsdaten ist keine ausschliessliche Frage der IT. Der Einsatz von IT-Mitteln im Zusammenhang mit den Verwaltungsdaten gewinnt jedoch stetig an Bedeutung. Verwaltungsdaten und vor allem vertrauliche Verwaltungsdaten bedürfen eines sorgfältigen und geregelten Umgangs, dies unabhängig davon, ob im Einzelfall für die Erstellung, Verarbeitung, Archivierung oder Versand IT-Mittel eingesetzt werden oder nicht.

2.2. Was sind Verwaltungsdaten

Verwaltungsdaten sind grundsätzlich alle Daten der Stadt, welche in einem Bezug stehen:

a) zu Verwaltungsvorgängen;
b) zu Kunden/Klienten-Beziehungen der Stadt;
c) zum Schulwesen;
d) zu Angestelltenbeziehungen der Stadt;
e) zu kooperierenden Amtsstellen ausserhalb der Stadtverwaltung;
f) zu Geschäftspartnern der Stadt;
g) zu Projekten.

2.3 Bearbeitung von Verwaltungsdaten mittels fremder IT-Lösungen

[1] Es ist untersagt, Verwaltungsdaten der Stadt auf fremden (z.B. privaten) Computern zu bearbeiten. Denn damit würde ein Wertbestand der Stadt

verzettelt auf Computersysteme, welche als unsicher gelten, weil diese nicht in das Sicherheitskonzept der Stadt eingebunden sind.

[2] Es ist zudem untersagt, Verwaltungsdaten auf Programmen zu verwalten, die nicht vom Amt für Telematik autorisiert wurden.

[3] Für die Lehrpersonen gelten ergänzend die Bestimmungen des aktuell gültigen, separaten Merkblattes „Bearbeitung von Verwaltungsdaten mittels fremder IT-Lösungen".

2.4 Was sind vertrauliche Verwaltungsdaten?

Vertrauliche Verwaltungsdaten sind speziell schützenswert. Dazu zählen insbesondere:

a) alle Daten der Stadt, welche nicht öffentlich zugänglich sind und welche in einem Bezug stehen zu Verwaltungsvorgängen der Stadt;
b) alle Daten, deren Informationsgehalt unter das Dienstgeheimnis fällt;
c) alle Daten, deren Informationsgehalt unter die Bestimmungen des Persönlichkeitsschutzes sowie der eidgenössischen und kantonalen Datenschutzgesetzgebung fällt.

2.5 Kopieren vertraulicher Verwaltungsdaten

[1] Das Kopieren vertraulicher Verwaltungsdaten ausserhalb der ordentlichen Verwaltungsprozesse ist untersagt.

[2] Die Mitnahme/Entfernung oder der Versand vertraulicher Verwaltungsdaten vom Arbeitsplatz ausserhalb der ordentlichen Verwaltungsprozesse ist untersagt. Eine solche Mitnahme bzw. Versand von Daten wird seitens der Stadt als Diebstahl vertraulicher Verwaltungsdaten interpretiert und kann strafrechtlich verfolgt werden.

2.6 Arbeiten ausser Haus

Eine ausnahmsweise Mitnahme vertraulicher Verwaltungsdaten ausserhalb des Arbeitsplatzdomizils bedarf einer Ermächtigung der vorgesetzten Stelle. Für die auf diesem Weg anvertrauten Wertbestände sind Sie persönlich verantwortlich (Laptop, Softwarelizenzen und Daten auf dem System).

2.7 Home Office Arbeitsplätze

[1] Home Office Arbeitsplätze sind vertraglich geregelte, stationär eingerichtete IT-Arbeitsplätze der Stadt am Wohnort einer oder eines Angestellten.

[2] Es gilt das separate Merkblatt „Home Office-Arbeitsplätze".

2.8 Datenspeicherung

Die Stadt kennt zwei Arten der Datenspeicherung (siehe auch grafische Darstellung auf nachfolgender Seite Abbildung 1):

1. Zentrale Daten

Diese Daten werden auf den zentralen Datenservern der Stadt gespeichert. Sie sind Gegenstand des Datensicherungskonzeptes und werden in einem geregelten Verfahren periodisch gesichert.

2. Lokale Daten

[1] Diese Daten werden lokal auf den Arbeitsplatzcomputern oder den mobilen Laptop Computern gespeichert. Diese Daten fallen an z.B. durch:

a) Das Einlesen von Floppys oder USB-Speicherchips (z.B. aus digitalen Fotokameras) auf Laptop oder Desktop Computer;
b) die Nutzung lokaler Programme auf Laptops im offline Betrieb (d.h. ohne Netzwerkverbindung).

[2] Diese Daten sind nicht Gegenstand des Datensicherungskonzeptes der Stadt. Für die Sicherheit und Verfügbarkeit lokaler Daten sind ausschliesslich die Anwendenden verantwortlich. Die Haltung lokaler Daten ist nur für kurze Zeit erlaubt. Lokale Daten mit verwaltungsrelevanter Bedeutung sind so schnell wie möglich in zentrale Daten zu überführen. Bitte beachten Sie speziell, dass lokale Daten unwiederbringlich verloren gehen, falls Ihr Computer neu aufgesetzt werden muss (z.B. nach einem technischen Defekt oder einem Befall durch Viren).

2.9 Organisation der Datenspeicherung

2.9.1 Ablage von Verwaltungsdaten

[1] Es wird zwischen folgenden Typen von Verwaltungsdaten unterschieden:

a) Verwaltungsdaten aus spezialisierten Applikationen (Finanzsystem, Bauverwaltung etc.);
b) Dateien/Dokumente zu Verwaltungsvorgängen (Word-Dokumente, Excel etc.);
c) Dateien/Dokumente zu Projekten;
d) E-Mails zu Verwaltungsvorgängen;
e) Projekte.

[2] Verwaltungsdaten aus spezialisierten Applikationen sind ausschliesslich in den zu diesem Zweck eingeführten Applikationen zu führen.

[3] Dateien / Dokumente zu Verwaltungsvorgängen sind als zentrale Daten innerhalb der zentralen Dateiablage (Laufwerk P:\) zu führen.

[4] E-Mails zu Verwaltungsvorgängen sind ebenfalls als zentrale Daten innerhalb des Laufwerkes P:\ zu führen. Zu diesem Zweck sind die

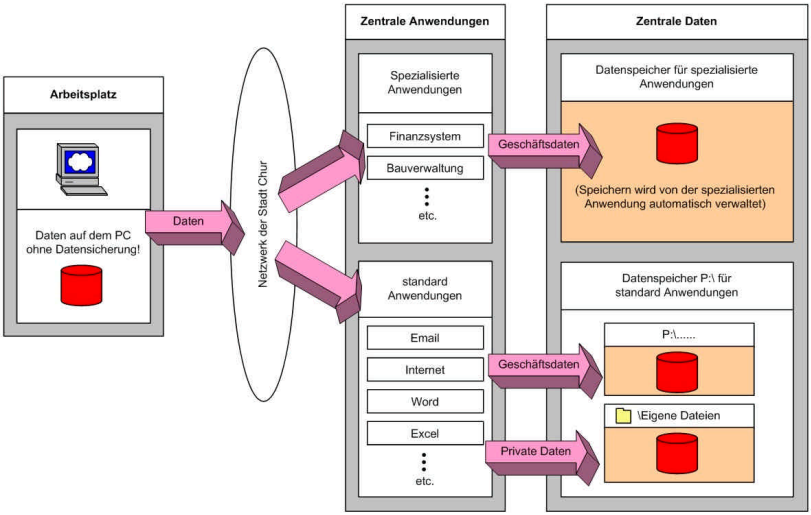
entsprechenden E-Mails aus dem Posteingang wie auch aus dem Ordner „gesendete Objekte“ in die zentrale Dateiablage (Laufwerk P:\) zu verschieben

2.9.2 Ablage von privaten Daten

[1] Für die privaten Daten steht ein eigener Bereich mit der Bezeichnung „Eigene Dateien“ zur Verfügung. Darin sind alle Daten mit privatem Charakter (gesendete u. empfangene E-Mails, Dateien und Dokumente etc.) abzulegen. Es ist ausdrücklich untersagt, private Daten in der geschäftlichen Mailbox oder auf dem Laufwerk P:\ zu speichern, ebenso Verwaltungsdaten in "Eigene Dateien". Der Speicherplatz wird mittels Kontingent für den Bereich „Eigene Dateien“ pro Anwender auf ein bestimmtes Maximum beschränkt.

[2] Wenn eine Mitarbeiterin oder ein Mitarbeiter die Stadt verlässt, werden ihm/ihr die privaten Daten aus dem Bereich „Eigene Dateien“ auf Wunsch auf einem Datenträger ausgehändigt. Ansonsten werden diese Daten nach spätestens 30 Tagen nach Austritt auf den zentralen Serversystemen unwiderruflich gelöscht.

Abbildung 1: Datenspeicherung



3. IT-Sicherheit

3.1. Anmeldenamen und Passwörter für IT-Anwendungen der Stadt

[1] Die Stadt hat in Ihren IT-Anwendungen verschiedene Massnahmen für den Schutz der Verwaltungsdaten implementiert. Sie als Angestellte oder Lehrperson werden mittels persönlichem Anmeldenamen und Passwort autorisiert, die Ihnen zugeteilten Anwendungen und Daten zu nutzen:

a) Sie sind verpflichtet, Anmeldenamen und Passwort geheim zu halten;
b) es ist nicht erlaubt, Anmeldenamen und Passwort von anderen Angestellten oder Lehrpersonen zu benutzen;
c) nach der Beendigung des Arbeitsverhältnisses sind auf Verlangen der Stadt alle Passwörter im Zusammenhang mit ihren Anwendungen an das Amt für Telematik bekannt zu geben.

[2] Wenn Sie einen Anmeldenamen oder ein Passwort vergessen haben, können Sie eine entsprechende Anfrage im IT-Supportcenter der Stadt erstellen.

3.2 Anmeldenamen und Passwörter für externe Anwendungen

Viele externe Anwendungen (z.B. im Internet) verlangen nach der Angabe eines Anwendernamens und nach der Eingabe eines Passwortes. Bei diesen Anwendungen ist nicht eindeutig ersichtlich, wer Zugang zu diesen Passwortdefinitionen hat, da die Vertrauenswürdigkeit und die Absicht des Anbieters oft unklar sind. Benutzen Sie bei externen Anwendungen (z.B. im Internet), welche von Ihnen die Definition eines Passwortes verlangen, niemals dasselbe Passwort wie für die IT-Lösungen der Stadt, denn Sie würden damit den "Schlüssel" zu Ihren internen Daten in unbekannte, externe Hände legen. Die unbekannte Stelle könnte diese Informationen benutzen, um nach einem Einbruch in das Netz der Stadt auf geschützte Daten zuzugreifen.

3.3 Beim Verlassen des Arbeitsplatzes

Melden Sie sich am System ab oder aktivieren Sie die Bildschirmsperre, wenn Sie Ihren Arbeitsplatz verlassen. Falls Sie mit einem Laptop ausser Haus arbeiten, so lassen Sie den Laptop niemals unbeaufsichtigt. Nach Arbeitsschluss ist die Arbeitsstation inkl. Bildschirm ordnungsgemäss abzuschalten.

3.4 Anschluss fremder Geräte an das Netz der Stadt

Der Anschluss fremder Geräte, welche nicht vom Amt für Telematik autorisiert wurden, an das Netz der Stadt ist untersagt (z.B. Modems, private Computer oder private Netzwerkkomponenten).

3.5 Virenschutz

3.5.1 Grundsätzliches

[1] Die Stadt setzt auf ihren IT-Systemen Schutzprogramme ein, um das Risiko der Einschleusung schädlicher Software (Software-Viren, Trojaner etc.) zu minimieren. Ein Virenbefall kann enorme Folgekosten verursachen in den Bereichen:

a) Restauration von Daten oder Programmen;
b) Arbeitsausfall (bedingt durch einen Stillstand der IT-Lösungen);
c) Korrektur von Datenmanipulationen.

[2] Ihr verantwortungsbewusster Umgang mit den IT-Lösungen der Stadt ist ein wesentlicher Beitrag zur Bewältigung dieser Risiken.

3.5.2 Schutzanwendungen der Stadt

Beim Start Ihres Computers wird automatisch ein Abwehrprogramm aktiviert. Dieses darf keinesfalls eigenhändig deaktiviert werden. Das Programm erkennt schädliche Software auf der Basis eines Vergleichs mit Mustern (sog. Virensignaturen) bekannter Viren. Beim Auftreten eines neuen Virus besteht das Restrisiko, dass die entsprechende Virensignatur dem Schutzsystem noch nicht bekannt ist. Um dieses Restrisiko zu minimieren, müssen:

a) die Virensignaturen so oft wie möglich auf jedem System aktualisiert werden; dies geschieht automatisch, wenn Ihr Computer am Netzwerk angeschlossen ist;
b) die möglichen Zugangstore für Daten (z.B. Floppys, CD's, USB-Speicherchips, etc.) so wenig wie möglich und mit grosser Eigenverantwortung nutzen.

3.5.3 Fremde Daten

[1] Als fremde Daten werden elektronische Informationen bezeichnet, welche von externen Stellen stammen.

[2] Werden diese Daten per E-Mail oder via Internet bezogen, kann davon ausgegangen werden, dass die stadteigenen zentralen Schutzsysteme, welche immer auf dem aktuellsten Stand der Virenerkennung gehalten werden, einen guten Schutz bieten.

[3] Werden diese Daten über einen Massenspeicherzugang eingelesen (Floppy, CD, USB-Speicherchip usw.) ist das Risiko höher. Dies gilt insbesondere für die mobilen Computer, da die Schutzsoftware nicht immer dem neusten Stand entspricht. Laptop Computer müssen so oft wie möglich (in der Regel täglich) an das Netz der Stadt angeschlossen werden, damit die automatische Aktualisierung der Virensignaturen durchgeführt werden kann. Falls Ihnen dies nicht möglich ist, so kontaktieren Sie bitte das IT-Supportcenter, damit eine individuelle Lösung gefunden werden kann.

3.5.4 Verhalten bei vermutetem Virenbefall

Wenn Sie auf Ihrem Computersystem ein ungewohntes Verhalten von Programmen oder fragwürdige Fehlermeldungen feststellen, so orientieren Sie unverzüglich das IT-Supportcenter, damit der Sachverhalt abgeklärt werden kann und Sie so schnell wie möglich wieder ein nutzbares System zur Verfügung haben.

3.6 Meldepflicht bei sicherheitstechnisch relevanten Vorkommnissen

[1] Das Amt für Telematik ist darauf angewiesen, dass es unverzüglich über alle sicherheitstechnisch relevanten Vorfälle informiert wird. Basierend auf Ihren Angaben können professionelle Stellen geeignete Schutzmassnahmen treffen, um entweder Schaden abzuwehren oder zu verhindern, dass ein bereits eingetretener Schaden sich weiter ausbreitet.

[2] Sie sind verpflichtet, sicherheitstechnisch relevante Vorfälle unverzüglich an das IT- Supportcenter zu melden. Dies ist ein wichtiger Beitrag Ihrerseits an einen möglichst sicheren IT-Betrieb der Stadt.

4. Nutzung der E-Mail Dienste

4.1 Grundsätzliches

Der E-Mail Dienst gehört zu den am meisten missbrauchten Kommunikationsarten in der modernen Geschäftswelt. Täglich werden unzählige E-Mails versendet, welche schädliche Computerviren transportieren. Eine unvorsichtige Nutzung des E-Mail Dienstes kann grossen Schaden verursachen. Im Zweifelsfalle hilft Ihnen das IT-Supportcenter bei der Beurteilung eines empfangenen Mails, welches Ihnen suspekt erscheint. Handeln Sie nach folgendem Grundsatz:
Ein vorsichtigerweise zuviel gelöschtes E-Mail kann mit vertretbarem Aufwand noch einmal gesendet werden. Ein unvorsichtigerweise geöffnetes E-Mail (oder dessen Beilage) kann grossen Schaden anrichten, der mit grossem Aufwand behoben werden muss.

4.2 Was sind suspekte E-Mails

[1] Ein E-Mail erscheint als suspekt, wenn:

a) Der Absender unbekannt ist und keinem Verwaltungsvorgang zugeordnet werden kann;
b) eine E-Mail-Beilage als ausführbares Programm beigefügt ist (d.h. der Dateiname endet mit .exe, .com, .vbs, .dll etc.);
c) der Absender zwar bekannt ist, aber die Betreffzeile keinen Bezug zu einem geschäftlichen Vorgang erkennen lässt.

[2] Suspekte E-Mails sind ohne zu öffnen sofort zu löschen.

4.3 Aufbewahrungspflicht/Speicherung verwaltungsrelevanter E-Mails (und Anhänge)

Als verwaltungsrelevante E-Mails gelten alle elektronischen Nachrichten, welche einen direkten Bezug zu Verwaltungsvorgängen bzw. zu den Geschäftsprozessen der Stadt haben und der Nachvollziehbarkeit dieser Vorgänge dienen. Diese E-Mails sind gemäss den Anweisungen unter 2.9 zu speichern.

4.4 Weiterleitung bei Abwesenheit

[1] Das E-Mail Programm bietet Ihnen verschiedene Möglichkeiten zur Handhabung einer Geschäftsabwesenheit. Sie können:

a) mittels einer Abwesenheitsregel E-Mails automatisch intern weiterleiten;
b) ihrer Stellvertretung den Lesezugriff auf Ihren E-Mail-Ordner temporär ermöglichen;
c) eine Abwesenheitsmeldung als automatische Antwort an den Sender des E-Mails schicken mit der Information, dass sein E-Mail nicht weitergeleitet wurde, wann Sie zurück sind und wer als Ihre Stellvertretung agiert.

[2] Falls Sie eine automatische Weiterleitung einrichten (mit dem Abwesenheitsassistenten des E-Mail Programms) beachten sie folgende Regeln:

a) Eine Weiterleitung an eine E-Mailadresse ausserhalb der Stadtverwaltung (z.B. Ihre private E-Mailadresse) ist untersagt, denn dies würde dazu führen, dass Informationen zu Verwaltungsvorgängen auf nicht vertrauenswürdigen und durch die Stadt nicht kontrollierbaren Computersystemen gespeichert werden. Für die Lehrpersonen der Stadt gelten zu diesem Punkt die Bestimmungen des aktuell gültigen, separaten Merkblattes für die Lehrpersonen.
b) Eine Weiterleitung an eine E-Mailadresse innerhalb der Stadtverwaltung (z.B. Ihre Stellvertretung) ist zulässig. Beachten Sie jedoch, dass eine Weiterleitung im Abwesenheitsfall aus Vertraulichkeitsüberlegungen nicht immer die optimale Lösung darstellt.

4.5 Umgang mit der persönlichen E-Mailadresse

Geben Sie Ihre geschäftliche E-Mailadresse nur an vertrauenswürdige Stellen und für geschäftliche Zwecke bekannt. Gehen Sie mit Ihrer E-Mailadresse bewusst um, ganz besonders im Internet. Jede Stelle, die Ihre E-Mailadresse kennt, kann Sie in beliebiger Intensität mit Werbemails („Spam“) belästigen, welche Ihren Posteingang und das Netzwerk der Stadt unnötig belasten.

4.6 Umgang mit E-Mail-Speicherplatz

Zur Optimierung der Netzwerkressourcen und für einen sinnvollen Umgang mit E-Mail-Speicherplatz weisen wir darauf hin, dass der zur Verfügung stehende Speicherplatz mittels Kontingenten limitiert ist. Die Zuteilung und Überwachung von Speicherplatz erfolgt durch das Amt für Telematik.

5. Nutzung des Internet

5.1 Eigene Identifikation im Internet

Bei der Nutzung des Internetzuganges der Stadt vertreten Sie die Stadt Chur im Internet. Sie repräsentieren also das Image der Stadt im Internet. Sie sind angehalten, Ihren korrekten Namen und die offizielle Adresse zu verwenden. Die Benutzung fremder Identifikationen (Pseudonyme) ist untersagt.

5.2 Bezug und Publikation von Informationen

[1] Als Angestellte oder Lehrpersonen der Stadt publizieren Sie keine Informationen:

a) welche von Dritten als anstössig, respektlos oder verletzend angesehen werden könnten;
b) welche willentlich missverständlich, verleumderisch oder falsch sind;
c) welche sexuellen oder extremistisch-politischen Inhalt haben.

[2] Sie greifen auch nicht auf Inhalte sexueller oder extremistisch-politischer Natur sowie strafrechtlich relevante Informationen zu. Falls Sie irrtümlich oder durch Fehlleitung auf solche Inhalte gestossen sind, können Sie das IT-Supportcenter orientieren, damit diese Inhalte mittels elektronischer Filter gesperrt werden.

5.3 Programme aus dem Internet

[1] Im Internet werden unzählige Anwendungsprogramme (z.B. als Gratisprogramme oder als „Shareware“) für jeden Zweck angeboten. Leider können diese Programme missbraucht werden, um "Spionageprogramme" (im Fachjargon „Trojaner“) oder Viren in ein Unternehmen einzuschleusen.

[2] Es ist Ihnen untersagt, in eigener Regie Programme aus dem Internet herunter zu laden und zu nutzen.

[3] Wenn Sie eine Software aus dem Internet für Ihren Arbeitsbereich nutzen wollen, so wenden Sie sich an das IT-Supportcenter. Dieses prüft Ihr Anliegen, den Anbieter, die Lizenzaspekte und die Sicherheit des gewünschten Programms.

5.4 Radio und Video im Internet

[1] Im Internet werden online Video- und Radioprogramme angeboten. Diese Angebote verursachen einen kontinuierlichen Datenstrom (im Fachjargon „Stream“) zwischen dem Anbieter und dem Zielarbeitsplatz. Durch die Nutzung solcher Streaming-Anwendungen kann das Netz der Stadt überlastet werden. Dadurch wird der Zugang zum Internet für alle Angestellten und Lehrpersonen unnötig erschwert.

[2] Die Nutzung von „Streams“ ist grundsätzlich untersagt. Falls Sie im Zusammenhang mit Verwaltungsvorgängen „Streams“ nutzen wollen oder müssen, wenden Sie sich an das IT-Supportcenter, damit eine spezifische Lösung erarbeitet werden kann, welche die anderen Angestellten und Lehrpersonen nicht behindert.

5.5 Publikationen von Informationen

Die Publikation von Informationen im Internet (z.B. auf Webservern, auf elektronischen Anschlag-Brettern, in Chat-Räumen etc.) unter Anwendung des Internet Zugangs der Stadt ist Ihnen untersagt.

6. Rechtliche Aspekte

6.1 Urheberrechte

[1] Daten und vom Amt für Telematik freigegebene Softwareprogramme unterliegen bestimmten Urheberrechten, Lizenzvereinbarungen oder anderen Schutzrechten. Sie sind verpflichtet, diese Bestimmungen einzuhalten, wenn diese im Zusammenhang mit von Ihnen genutzten Daten oder Programmen aus dem Internet stehen.

[2] Wenn Sie Informationen aus dem Internet kopieren, müssen Sie, wenn möglich, die damit verbundenen Schutzrechte ebenfalls mitkopieren (z.B. die Bestimmungen zum Urheberrecht).

[3] Die Nutzungsrechte an Erfindungen, Entdeckungen, Ideen, Konzepten, Methoden und Softwareprogrammen, die vom städtischen Personal im Zusammenhang mit IT- Lösungen der Stadt erarbeitet wurden, sind Eigentum der Stadt.

6.2 Verträge über elektronische Medien

Auf der Basis der neuen elektronischen Medien (www.-Dienste im Internet) können juristisch gültige Verträge abgeschlossen werden. Gleichzeitig sind jedoch viele Angebote im Internet mit ungenügender Transparenz dargestellt (z.B. ist der Anbieter unbekannt oder unklar, die allgemeinen Vertragsbestimmungen sind unsichtbar, Nutzungsbestimmungen sind unklar oder unverständlich etc.).

a) Sie haben zu berücksichtigen, dass Sie nur im Rahmen Ihrer Befugnis (u.a. Kompetenzregelung) für die Stadt rechtsverbindliche Verträge eingehen können.
b) Sie sind dazu verpflichtet, Angebote in elektronischer Form mit grosser Sorgfalt zu behandeln und seriös zu prüfen. Wenn Sie auf ein Angebot via elektronisches Medium eintreten, so haben Sie sicherzustellen, dass alle Geschäftsbedingungen (Lieferant, Vertragsbestimmungen, allg. Geschäftsbedingungen etc.) bekannt und nachvollziehbar vorhanden sind (z.B. als Papierausdruck).

6.3 E-Mail Fusszeilentext

Die Stadt ordnet der E-Mail-Kommunikation mit Ausnahme von Vertragsabschlüssen gemäss Ziff. 6.2 vorstehend keine rechtsverbindliche Wirkung zu. Dem Empfänger muss dies klar kommuniziert werden. Deshalb wird zu jedem neu generierten E-Mail automatisch eine stadtspezifische Fusszeile generiert.

7. Private Nutzung von IT-Lösungen der Stadt

7.1 Grundsätzliches

Die Bereitstellung und der Betrieb ihrer IT-Lösungen sind für die Stadt mit namhaften Kosten verbunden. Demzufolge sind diese Lösungen ausschliesslich für geschäftliche Zwecke vorgesehen.

7.2 Ausnahmen

[1] Im Sinne einer grosszügigen Haltung gegenüber dem städtischen Personal verzichtet die Stadt auf ein grundsätzliches Verbot der privaten Nutzung ihrer IT-Lösungen.
[2] Zulässig ist eine gelegentliche, nicht regelmässige private Nutzung, solange diese den regulären IT-Betrieb nicht stört und Ihre eigene Auftragserfüllung und die der anderen Angestellten und Lehrpersonen nicht behindert.
[3] Die nachfolgenden Abschnitte geben im Detail Auskunft, welche Anwendungen für den gelegentlichen privaten Gebrauch zugelassen sind und welche ausdrücklich untersagt sind.
[4] Bei begründetem Verdacht auf Missbrauch durch die private Nutzung der IT-Lösungen der Stadt behält sich das Amt für Telematik das Recht vor, technische Kontrollen anzuordnen. Dabei hält sich das Amt für Telematik an die einschlägigen Vorschriften zum Daten- und Persönlichkeitsschutz.

7.3 Programme

[1] Für die gelegentliche private Nutzung zugelassen sind folgende Standard-Anwendungen: Word, Excel, Powerpoint, Outlook/E-Mail, elektronisches Telefonbuch, Internet-Explorer, Programme für die Bildbearbeitung.

[2] Für alle anderen Anwendungen ist die private Nutzung untersagt.

[3] Das Kopieren von Programmen der Stadt für private Zwecke ist untersagt.

7.4 Internet Nutzung

[1] Die gelegentliche private Nutzung des Internet Zugangs zum Zweck der Informationsabfrage ist zulässig. Auch für die private Nutzung sind die Bestimmungen gemäss Kapitel 5 einzuhalten.

[2] Der Download umfangreicher Datenbestände (z.B. grösser als 1 MByte) für die private Nutzung ist verboten, denn dies belastet den Internetzugang zu stark und behindert die übrigen Angestellten und Lehrpersonen in ihrer Arbeit.

7.5 E-Mail

[1] Die gelegentliche private Nutzung der E-Mail Anwendung ist zulässig. Auch für die private Nutzung sind die Bestimmungen gemäss Kapitel 4 einzuhalten.

[2] Sie sind verpflichtet, Ihre privaten Nachrichten in einem separaten Ordner zu speichern (siehe dazu auch Kapitel 2.9).

7.6 Private Daten

[1] Als private Daten werden alle Daten bezeichnet, welche nicht im Zusammenhang mit der geschäftlichen Nutzung der IT-Lösungen der Stadt stehen.

[2] Für die Speicherung privater Daten (z.B. Anhänge zu privaten E-Mails) ist gemäss den Vorgaben des Kapitels 2.9 zu verfahren.

[3] Das Laden privater Daten auf Systeme der Stadt (z.B. ab Floppy, CD-Rom, USB-Memorystick etc.) ist untersagt, denn dieser Vorgang würde die zentralen Sicherheitseinrichtungen zum Schutz vor Viren und anderer schädlicher Software teilweise umgehen und ein zusätzliches Risikopotenzial darstellen. Private Daten dürfen nur über den E-Mailweg in die IT-Systeme der Stadt geladen werden.

7.7 Private Programme

[1] Der Einsatz privater Programme auf IT-Systemen der Stadt ist untersagt.

[2] Als private Programme werden alle Programme bezeichnet, welche nicht vom Amt für Telematik der Stadt installiert oder zur Nutzung autorisiert wurden.

7.8 Rechtsanspruch aus privater Nutzung

Durch die private Nutzung der IT-Lösungen der Stadt entstehen für das städtische Personal keinerlei Rechtsansprüche gegenüber der Stadt. Speziell übernimmt die Stadt keinerlei Haftung für die Verfügbarkeit, die Sicherheit oder die Vertraulichkeit gegenüber Dritten bezüglich Ihrer privaten Daten auf Systemen der Stadt.

7.9 Datenschutz, Schutz der Privatsphäre

Die Stadt hält gegenüber dem städtischen Personal auch bezüglich privater Daten die Bestimmung der Schweizerischen Datenschutzgesetzgebung und des Persönlichkeitsschutzes ein.