Stadt Zürich

Sicher im Internet und in den neuen Medien

Social Media haben unser Kommunikationsverhalten stark verändert. Diese Broschüre umfasst Leitlinien für die Mitarbeitenden und Tipps der «einfach SICHER»-Kampagne für den sicheren Umgang mit Daten.

Ob Facebook, Twitter oder Xing – Social Media begleiten uns nicht nur im Privat-, sondern zunehmend auch im Geschäftsleben. Die Leitlinien im ersten Teil dieser Broschüre weisen Sie auf die wichtigsten Punkte zum sicheren und angemessenen Benutzen von Social Media hin.

Abgesehen von Social Media ist aber auch bei der Nutzung anderer Medien Vorsicht geboten. Um Sie für den sicheren Umgang mit Daten zu sensibilisieren, hat die OIZ die Kampagne «einfach SICHER» durchgeführt. Die gesammelten Tipps und Informationen zu Sicherheitsthemen finden Sie ebenfalls in dieser Broschüre.

Impressum
Herausgeberin: Stadt Zürich

Titelbild: Stadt Zürich
Konzept und Gestaltung: Prime
Druck: GeoPrint-Shop, Zürich

Papier: RecyStar Polar hochweiss

Bezugsquelle:
Download als PDF von
www.stadt-zuerich.ch/socialmedia

Fragen zum Thema
Informationssicherheit:
Fachstelle Informationssicherheit
itsec@zuerich.ch
044 412 96 06

Zürich, Dezember 2012

Inhaltsverzeichnis

Umgang mit Social Media

Leitlinien für die Mitarbeitenden der Stadt Zürich
Social Media unterscheiden sich von traditionellen Massenmedien in erster Linie durch ihre Möglichkeit zur Interaktivität («Dialog statt Monolog»). Sie lassen sich aus unserem privaten und beruflichen Alltag nicht mehr wegdenken.

Diese Leitlinien richten sich an alle städtischen Mitarbeitenden, die auf Social-Media-Plattformen aktiv sind, und sollen bei der Nutzung der Plattformen unterstützen sowie auf mögliche Gefahren und Risiken, besonders auch im Zusammenhang mit der Stadt Zürich als Arbeitgeberin, sensibilisieren.

1.

Offizielle Auftritte der Stadt in Social Media

Die städtischen Social-Media-Kanäle und -Auftritte werden von explizit damit beauftragten und dafür autorisierten Mitarbeitenden betreut.

2.

Social Media am Arbeitsplatz

Die Stadt Zürich als Arbeitgeberin setzt bei der Nutzung von Social Media grundsätzlich auf die Eigenverantwortung jeder Mitarbeiterin und jedes Mitarbeiters.
Der private Gebrauch von Social Media darf die dienstlichen Aufgaben nicht beeinträchtigen.

6.

Urheber- und Nutzungsrechte

Keine Inhalte (Texte, Bilder, Audio- und Videofiles) verwenden, bei denen das Urheber- oder Nutzungsrecht verletzt wird.

7.

Das Netz vergisst nie und nichts

Einmal publizierte Daten, insbesondere auch Bildmaterial, lassen sich kaum mehr vollständig aus dem Internet löschen und können unkontrolliert weiterverbreitet werden.

3.

Geheimhaltungspflicht und Datenschutz

Als Mitarbeitende der Stadt Zürich sind Sie an das Amtsgeheimnis gebunden.

Vertrauliche Informationen (z. B. noch nicht veröffentlichte Entscheide, Personendaten usw.) dürfen nicht publiziert werden.

4.

Privat vs. Business

Auch als Privatpersonen tragen Mitarbeitende der Stadt Zürich Verantwortung gegenüber ihrer Arbeitgeberin.

Besonders sorgsam ist mit unternehmensbezogenen Informationen umzugehen (Amtsgeheimnis).

5.

Eigene Kennwörter benutzen und keine Geschäftskontakte verwenden

Aus Sicherheitsgründen sind zwingend andere Passwörter zu verwenden als am Arbeitsplatz. Berufliche Kontakte (z. B. aus Outlook oder Mobiltelefon) dürfen nicht in Social-Media-Profile importiert werden.

8.

Den Anstand wahren

Keine beleidigenden, diskriminierenden, rassistischen oder vulgären Beiträge publizieren.

9.

Stadt Zürich in Social Media

Die Stadt Zürich kann auch auf Social-Media-Kanälen und -Profilen von Dritten zum Thema werden. Die Kommunikationsabteilungen nehmen gerne Hinweise zu Diskussionen über die Stadtverwaltung oder über ihre Dienstleistungen entgegen.

10.

Unsicher?

Bitte wenden Sie sich bei Unsicherheiten an Ihre/n Vorgesetzte/n.

Social Media – was ist das?

Social Media bezeichnet Online-Plattformen, die zur Kommunikation, also zu einem Austausch von Meinungen, Eindrücken und Erfahrungen dienen (Beispiele: Facebook, Google+, Xing, LinkedIn), oder mit denen sich Wissen, Inhalte und Informationen (Texte, Bilder, Audio- und Videofiles) generieren, bearbeiten und teilen lassen (Beispiele: Wikipedia, Youtube/Vimeo, Twitter, Flickr, Pinterest, Instagram).

Auch Blogs, Chats, Foren und die Kommentarfunktion in Online-Zeitungen gehören zur Welt von Social Media.

Mit Social Media können sich Menschen vernetzen; mit ihrem Freundes- und Bekanntenkreis, aber auch mit Fremden, mit denen sie Interessen teilen. Social Media ermöglichen eine einfache Kontaktpflege, weltweite Kommunikation und ein rasches Austauschen von Inhalten ohne grosse technische Hürden. Social Media haben die Kommunikation verändert. Informationen und Bilder können durch Verlinken und gegenseitiges Teilen mit hoher Geschwindigkeit und grosser Reichweite verbreitet werden.

Social Media & die Stadt Zürich

Social Media bieten der Stadt Zürich eine weitere Möglichkeit, sich mit der Bevölkerung auszutauschen und ihren Informationsauftrag umfassender zu erfüllen. Die Stadt Zürich wie auch einzelne Organisationseinheiten oder Projekte sind mit eigenem Profil in Social Media vertreten. Die offiziellen Aktivitäten der Stadtverwaltung sind verzeichnet unter www.stadt-zuerich.ch/socialmedia.

Für die Publikation von Inhalten sowie die Moderation von Kommentaren oder Anregungen in den offiziellen städtischen Social-Media-Kanälen sind explizit damit beauftragte und dafür autorisierte Mitarbeiterinnen und Mitarbeiter verantwortlich.

Social Media & die Mitarbeitenden

Bei der privaten Nutzung von Social Media setzt die Stadt Zürich als Arbeitgeberin auf die Eigenverantwortung ihrer Mitarbeiterinnen und Mitarbeiter. Grundsätzlich sind private Angelegenheiten in der Freizeit zu erledigen. Die Nutzung von Social Media zu privaten Zwecken darf den Dienstbetrieb und die Erfüllung der dienstlichen Aufgaben nicht beeinträchtigen.

Die Stadt Zürich vertraut bei der Nutzung von Social Media auf Ihre Eigenverantwortung als Mitarbeiterin oder Mitarbeiter.

Mitarbeitende sind wichtige Botschafterinnen und Botschafter
Die Mitarbeiterinnen und Mitarbeiter der Stadt Zürich repräsentieren die Zürcher Stadtverwaltung, ihre Angebote und ihre (Dienst-)Leistungen. Sie tragen massgeblich zum positiven Image der Stadtverwaltung bei.

Sie sind wichtige Botschafterinnen und Botschafter der Stadt Zürich. Helfen Sie mit, unser positives Image zu fördern und zu verstärken.

Die Mitarbeitenden der Stadt Zürich sind eingeladen, die offiziellen Seiten auch privat zu «liken», Fan zu werden, ihnen zu «followen» oder Inhalte zu «liken» oder zu «teilen».

Rechtliches
Die Stadt Zürich achtet und befürwortet die freie Meinungsäusserung ihrer Mitarbeitenden und schätzt sachliche und konstruktive Dialoge auch in Social Media.

Die Mitarbeitenden der Stadt Zürich tragen auch als Privatpersonen Verantwortung gegenüber ihrer Arbeitgeberin. Besonders sorgsam ist mit vertraulichen, internen oder (noch) nicht öffentlich publizierten Informationen umzugehen (Amtsgeheimnis). Im Zweifelsfall ist mit der/dem Vorgesetzten Rücksprache zu nehmen.

Keine vertraulichen, internen oder (noch) nicht öffentlich publizierten Informationen in Social Media veröffentlichen!

IT-Sicherheit

Aus Sicherheitsgründen ist es zwingend, für private Social-Media-Profile andere Passwörter einzusetzen als am Arbeitsplatz.

Für die Registrierung und zur Kommunikation müssen private Kontaktangaben eingesetzt werden. Auch dürfen berufliche Kontakte (z. B. aus Outlook oder Mobiltelefon) nicht in Social-Media-Profile importiert werden. Die Geschäfts-E-Mail-Adresse darf ausschliesslich dann verwendet werden, wenn die Internetseite geschäftlichen Zwecken dient.

Für private Accounts und Profile keine städtischen Passwörter und E-Mail-Adressen verwenden!

Insbesondere gelten folgende Gesetze auch in Social Media:

- Persönlichkeitsrecht (z. B. beleidigende, rufschädigende und unwahre Aussagen zu einer Person, Recht am eigenen Bild)
- Urheberrecht (Publikation und Weiterverbreitung von geschützten Texten, Bildern, Audio- oder Videofiles)
- Geheimhaltungsvorschriften (Datenschutz, Amts- und Geschäftsgeheimnis)

Zu nicht zulässigen Handlungen gehören:

- Missbrauch der geschützten Marke «Stadt Zürich» (private Seiten oder Profile dürfen nicht den Anschein machen, es handle sich um ein offizielles Engagement der Stadt Zürich)
- Aufforderung zu Gewalt gegen Personen, Institutionen oder Unternehmen, Rassismus, Diskriminierung und Hetzkampagnen
- Publizieren von pornografischen Inhalten
- Missbrauch der Kommentarfunktion als Werbefläche
- Urheber- und Persönlichkeitsrechte gelten auch in Social Media!

Stolpersteine

Die Benutzung von Social-Media-Plattformen ist einfach und Profile sind rasch erstellt. Einmal veröffentlichte Daten und Bildmaterialien lassen sich aber kaum mehr vollständig aus dem Internet löschen und können unkontrolliert weiterverbreitet werden.

Bilder

In Social Media wird oft mit Bildern und Videos kommuniziert. Gerade hier gilt besondere Vorsicht. Die meisten Bilder sind urheberrechtlich geschützt und es gilt das Recht am eigenen Bild: Fotos von Personen dürfen nicht ohne deren Einwilligung publiziert werden.

Das Netz vergisst nichts – einmal publizierte Daten lassen sich kaum mehr löschen!

Netikette

Hinter den virtuellen Persönlichkeiten im Netz stehen Menschen. Auch in Social Media gelten Anstandsregeln. In Diskussionen kann durchaus kontrovers argumentiert werden, jedoch mit Respekt vor den anderen Beteiligten, sachlich und ohne persönliche Angriffe.

Die Stadt Zürich in Social Media

Die Stadt Zürich kann auch auf Social-Media-Kanälen und -Profilen von Dritten zum Thema werden.

Die Kommunikationsabteilungen nehmen gerne Hinweise zu Diskussionen über die Stadtverwaltung oder über ihre Dienstleistungen entgegen.

Passwörter

Sichere Passwörter sind wichtig, weil sie die Schlüssel zu Ihren persönlichen Daten sind! Gelingt es einem Hacker, Ihr Passwort zu knacken, kann er auf alle Systeme zugreifen, auf denen Sie Zugriffsberechtigung haben. Zudem kann er sich als Sie ausgeben (sogenannter Identitätsdiebstahl).

Gemäss dem städtischen Passwortreglement müssen Passwörter mindestens 8 Zeichen lang sein, Gross- und Kleinbuchstaben sowie Zahlen oder Sonderzeichen enthalten.

Das Wichtigste in Kürze:

- Geben Sie Ihre Passwörter weder Mitarbeitenden, noch Stellvertretungen oder Systemverantwortlichen bekannt.
- Sperren Sie Ihren PC bei Abwesenheit vom Arbeitsplatz.
- Ändern Sie Passwörter regelmässig und wechseln Sie diese sofort bei Verdacht auf Missbrauch.
- Benutzen Sie verschiedene Passwörter für unterschiedliche Anwendungen.
- Verwenden Sie geschäftlich und privat andere Passwörter.
- Schreiben Sie Passwörter am besten gar nicht auf, oder nur an einem geschützten Ort (Passwort Safe).
- Wechseln Sie Initialpasswörter beim ersten Gebrauch.

Viren und Phishing

Viren und sonstige bösartige Software werden am häufigsten auf einem der folgenden drei Wege verbreitet:

- In E-Mails, indem ein verseuchter E-Mail-Anhang versandt wird
- Über USB-Sticks, die von einem infizierten Computer zum nächsten weitergereicht werden
- Über Internet-Webseiten, die mit einer Schadsoftware ausgerüstet sind (sogenannter Drive-By-Download)

Phishing ist eine Methode von Betrügern, um sich Informationen von ihren Opfern zu beschaffen, die zur persönlichen Bereicherung eingesetzt werden können. Beispiele solcher Informationen sind Passwörter, Streichlisten, Vertrags- oder Kontonummern von Online-Diensten wie beispielsweise E-Banking. Phishing-Angriffe erfolgen oft via E-Mails, in denen Benutzer mit möglichst glaubhaften Geschichten dazu gebracht werden sollen, dem Absender diese vertraulichen Informationen auszuhändigen.

Eine andere Möglichkeit besteht darin, Opfer auf eine präparierte Website zu locken. Dort kopiert ein Trojaner unbemerkt Informationen vom Computer des Opfers und stellt sie dem Betrüger zu.

Besonders beliebt sind Phishing-Angriffe über Facebook, z. B. über Chat (URL im Chat-Text) oder Freundeslisten.

Phishing E-Mails lassen sich am ehesten an Rechtschreibfehlern und dubiosen Absenderadressen erkennen. Doch auch Phishing-Mails werden immer professioneller gemacht und sind zunehmend schwer zu identifizieren.

Das Wichtigste in Kürze:

- Seriöse Unternehmen fragen nie per E-Mail nach persönlichen Daten.
- Misstrauen Sie E-Mails, deren Absender Sie nicht kennen oder deren Inhalt Ihnen verdächtig vorkommt.
- Fahren Sie mit dem Mauszeiger über die Internet-Adresse in der E-Mail, ohne zu klicken; so sehen Sie, auf welche Website der Link führt.
- Öffnen Sie bei solchen E-Mails nie ein angehängtes Dokument oder Programm und wählen Sie keine darin angegebenen Links.
- Öffnen Sie nur Anhänge aus vertrauenswürdigen Quellen und nach vorgängiger Prüfung mit einer aktuellen Virenschutz-Software.
- Ignorieren Sie E-Mail-Aufforderungen, Ihr Passwort zu ändern.
- Öffnen Sie keine Anhänge, die zwei Endungen aufweisen (z. B. foto.jpg.vbs).

Privatsphäre im Internet

Das Internet kennt kein Vergessen! Seien Sie sich bewusst, dass Informationen und Bilder, die Sie einmal im Netz veröffentlicht oder per Mobiltelefon weitergeschickt haben, von anderen Personen ausgenutzt oder missbraucht werden können. Informationen bleiben selbst dann meist noch irgendwo erhalten, wenn Sie diese wieder gelöscht haben.

So ist z. B. das unwiderrufliche Löschen eines Benutzerkontos auf sozialen Plattformen wie Facebook praktisch nicht möglich. Meist werden solche Profile nur deaktiviert. Die Betreiber der Plattform können aber weiterhin auf alle Ihre Daten zugreifen.

Bevor Sie persönliche Informationen ins Internet stellen, überlegen Sie sich deshalb genau, ob Sie diese auch Ihren Nachbarn erzählen oder zeigen würden. Falls nein, seien Sie zurückhaltend und verwenden Sie für Ihre Online-Präsenz ein Pseudonym (einen Fantasienamen).

Das Wichtigste in Kürze:

- Seien Sie zurückhaltend beim Veröffentlichen und Freigeben privater Daten, Informationen und Aktivitäten im Internet und per Mobiltelefon.
- Geben Sie in Online-Formularen nur die absolut nötigen Informationen an. Je mehr Daten Sie preisgeben, desto eher können Internet-Anbieter ein Nutzerprofil von Ihnen erstellen.
- Veröffentlichen Sie keine Inhalte, die Ihnen einmal peinlich sein könnten (z. B. Fotos aus der Jugendzeit).
- Verzichten Sie in Benutzerprofilen auf Angaben über Ihre konkrete geschäftliche Funktion oder Ihre Aufgaben.
- Verraten Sie Ihre Freunde nicht! Veröffentlichen Sie keine Fotos oder Daten Ihrer Freunde mit deren Namen ohne deren explizite Einwilligung.
- Laden Sie keine Adressbücher von Ihrem Computer oder Mobilgerät ins Internet oder in Apps hoch.

Vertrauliche Informationen

Geschäftliche Informationen, die Sie an Ihrem Arbeitsplatz bearbeiten, dürfen nur berechtigten Personen zugänglich sein. Sorgen Sie deshalb auch beim kurzzeitigen Verlassen Ihres Arbeitsplatzes dafür, dass Unberechtigte keinen Einblick in für sie nicht vorgesehene Informationen erhalten.

Zeigen Sie auch auf dem Arbeitsweg oder in der Freizeit (z. B. im Tram oder Restaurant) und bei Gesprächen mit Freunden und Dritten die nötige Zurückhaltung, wenn es um stadtinterne Angelegenheiten geht.

Das Wichtigste in Kürze:

- Verwenden Sie konsequent die Bildschirmsperre bei Abwesenheit vom Arbeitsplatz.
- Holen Sie ausgedruckte vertrauliche Informationen umgehend vom Drucker ab.
- Entfernen Sie im Sitzungszimmer Flip-Chart-Blätter mit vertraulichen Informationen.
- Melden Sie sich bei Arbeitsschluss vom internen Netzwerk ab («Herunterfahren», nicht «Stromsparen»).
- Schliessen Sie vertrauliche Akten und Datenträger (DVDs, USB-Sticks) ein.
- Werfen Sie vertrauliche Papierdokumente nicht ins Altpapier, sondern schreddern Sie diese.
- Verschlüsseln Sie vertrauliche Informationen, die Sie an Dritte übermitteln oder auf einem mobilen Gerät abspeichern.

Smartphones

Ob mit Smartphones oder mit Tablet-PCs, fast sämtliche Funktionen eines PCs können auch mobil genutzt werden. Da ist es nicht weiter erstaunlich, dass mobile Geräte vermehrt für die geschäftliche Kommunikation genutzt werden. Mit dem Austausch sensibler Daten über mobile Geräte tritt auch deren Sicherheit vermehrt in den Fokus.

Für die Sicherheit der Smartphones und Tablet-PCs gilt das gleiche wie für reguläre PCs. Schützen Sie jedes Gerät mit einem Passwort (keine einfachen Zahlenreihen!), nutzen Sie wenn möglich keine öffentlichen WLANs (ohne Benutzer-ID und Passwortschutz) um im Internet zu surfen, aktualisieren Sie regelmässig Ihr Backup. Informieren Sie den Service Desk bei Verlust oder Diebstahl Ihres mobilen Geräts, falls Sie dieses über AirSync mit Ihrem Postfach synchronisieren.

Besonders vorsichtig sollten Sie beim Herunterladen von Apps sein. Manche App-Anbieter greifen auf die Daten Ihres mobilen Geräts zu, ohne dass eine Notwendigkeit dafür besteht. So können Anbieter zum Beispiel bequem an Ihre Kontaktdaten gelangen und diese nutzen und weiterreichen. Dasselbe gilt übrigens für Social Networks. Verzichten Sie deshalb darauf, Kontaktdaten (Adressbuch, Outlook-Kontakte) mit Facebook, Twitter und anderen Netzwerken abzugleichen.

Das Wichtigste in Kürze:

- Schützen Sie Ihr Smartphone mit einem Passwort aus 4–6 Ziffern. Vermeiden Sie einfache Zahlenreihen wie 1111 oder 123456.
- Aktivieren Sie die automatische Sperre, die sich bei Nichtgebrauch des Smartphones selbständig einschaltet.
- Lassen Sie Ihre SIM-Karte sofort sperren, wenn Sie Ihr Smartphone verlieren oder es gestohlen wurde.
- Installieren Sie Apps zum Schutz vor Viren und Malware (Schadprogramme). Achten Sie darauf, dass die Software aus einer sicheren Quelle stammt.
- Das Synchronisieren von Adressbüchern mit Social-Networks und anderen Internet-Plattformen ist beliebt. Seien Sie sich bewusst, dass die AnbieterInnen der Plattformen die Kontakte kopieren und für ihre Zwecke verwenden und weiterreichen können.

Cloud-Dienste

Eine «Cloud» (deutsch: Wolke) beschreibt die von einem Anbieter online zur Verfügung gestellte Hardware und Software. Die Anwendungen und Daten befinden sich dann nicht mehr auf dem lokalen Gerät, sondern in der «Wolke». Beispiele dafür sind «Dropbox» oder «iCloud».

Der Vorteil von Cloud-Diensten ist, dass mehrere Personen von unterschiedlichen lokalen Netzwerken auf die Daten in der Cloud zugreifen können.

Cloud-Dienste haben aber auch ihre Nachteile: Die Server der Anbieter sind geografisch oft global verstreut. Das kann rechtliche Unklarheiten und Sicherheitsprobleme mit sich bringen. Wenn ein Anbieter seinen Hauptsitz beispielsweise in den USA hat, darf die amerikanische Regierung sämtliche Daten jederzeit einsehen.

Als positiv und empfehlenswert hervorheben kann man den Schweizer Cloud-Dienst «SecureSafe» von der Firma DSWiss, bei dem die Daten beim Kunden so verschlüsselt sind, dass niemand anderes darauf zugreifen kann.

Das Wichtigste in Kürze:

- Seien Sie zurückhaltend mit dem Speichern persönlicher, sensibler Daten in Clouds und speichern Sie dort nie unter Datenschutz stehende Daten.
- Prüfen Sie die Sicherheitsbedingungen eines Anbieters, bevor Sie sich für einen Dienst entscheiden: Daten sollten innerhalb der Cloud verschlüsselt übermittelt werden.
- Prüfen Sie, ob der Anbieter einem Sicherheitsabkommen zugestimmt hat (z. B. «Safe-Harbor-Abkommen»).
- Meiden Sie gratis Cloud-Angebote. Deren Anbieter verdienen ihr Geld oft mit der inhaltlichen Analyse der Daten ihrer Nutzer, um sie danach für Werbespam zu verwenden.
- Machen Sie Sicherheitskopien Ihrer Daten auf Ihrem lokalen Computer, damit Ihre Daten bei einem Serverausfall des Cloud-Dienstes sicher sind.