reformierte
kirche oberglatt

Datenschutz ICT – Nutzungsweisung

Inhaltsverzeichnis

Vorbemerkung

Das vorliegende Dokument enthält in der Praxis übliche Regelungen hinsichtlich des Umgangs mit ICT-Mitteln und -Systemen im dienstlichen Kontext. Es kann einer Kirchgemeinde als Richtschnur und Vorlage für die Einführung entsprechender Pflichten dienen.

Einleitung

Worum geht es?

Die vorliegende ICT-Nutzungsweisung hat zum Ziel, den Mitgliedern der Kirchenpflege sowie den Mitarbeiterinnen und Mitarbeitern verständliche und nachvollziehbare Vorgaben bei der Nutzung von ICT-Mitteln und -Systemen, die im Zusammenhang mit der Tätigkeit innerhalb der Kirchgemeinde verwendet werden (nachfolgend ICT-Mittel), zu geben. Die Weisung dient damit der Einhaltung von Vorgaben des Datenschutzes und insbesondere der Informationssicherheit und der Vermeidung von damit einhergehenden Risiken für die Kirchgemeinden.

Ein sorgsamer und verantwortungsvoller Umgang mit ICT-Mitteln trägt dazu bei, einen störungsfreien und sicheren Betrieb der Kirchgemeinde zu garantieren.

Grundsätze der Informationssicherheit

Die Informationssicherheit dient dem Schutz der Vertraulichkeit, der Verfügbarkeit sowie der Integrität der innerhalb der Kirchgemeinde bearbeiteten Informationen und Datenbestände.

Rechtliche Einordnung des Dokuments

Die ICT-Nutzungsweisung gilt für alle Mitglieder der Kirchenpflege sowie für alle Pfarrerinnen, Pfarrer, Angestellten sowie für alle Freiwilligen der Kirchengemeinden und ist in deren Arbeitsalltag stets zu befolgen.

Die in der Weisung enthaltenen Bestimmungen orientieren sich an den anwendbaren und massgebenden Vorgaben im Bereich des Datenschutzes und der Informationssicherheit. Das sind namentlich das Gesetz über die Information und den Datenschutz (IDG, LS 170.4), die dazugehörige Verordnung (IDV, 170.41) sowie das Kirchlichen Datenschutz-Reglement (LS 180.7). Weiter werden die relevanten Bestimmungen der Personalverordnung der Evangelisch-reformierten Landeskirche des Kantons Zürich (LS 181.40) sowie der zugehörigen Vollzugsverordnung (LS 181.401) berücksichtigt.

Verantwortlichkeiten

Funktion	Verantwortlichkeiten
Kirchenpflege (Exekutive)	Die Kirchenpflege als Behörde trägt die Gesamtverantwortung für die Einhaltung der rechtlichen Vorgaben und damit auch für den Datenschutz und die Informationssicherheit. Sie sorgt für die Umsetzung der allgemeinen Vorgaben innerhalb der Organisation und stellt sicher, dass die notwendigen finanziellen und personellen Ressourcen vorhanden sind, damit die Kirchgemeinde datenschutzkonform handelt, und kontrolliert die Umsetzung des Datenschutzes und der Informationssicherheit kontinuierlich.
Ansprechperson für Datenschutzfragen	Die Ansprechperson für Datenschutzfragen ist auch bei Fragen zur Informationssicherheit und Nutzung von ICT-Mitteln die innerhalb der Landeskirche zuständige Ansprechperson. (Für die Beschreibung und Pflichten der Rolle siehe das Datenschutz-Handbuch, Ziffer 2.)
Ansprechperson für Informationssicherheit	Falls die Kirchgemeinde intern oder extern eine für Informationssicherheit zuständige Person bezeichnet hat, so ist diese die zuständige Anlaufstelle für sämtliche damit zusammenhängende Fragen (anstelle der Ansprechperson für Datenschutzfragen, siehe hiervor). Die Person erteilt die Autorisation für den Einsatz von ICT-Systemen sowie anderweitig notwendige Bewilligungen aus Perspektive der Informationssicherheit. Die Person nimmt eine beratende Funktion wahr. Sie ist intern bekannt zu machen.
Mitarbeiterin oder Mitarbeiter	Jede Mitarbeiterin und jeder Mitarbeiter sorgt dafür, dass die Grundsätze des Datenschutzes sowie der Informationssicherheit und die definierten Prozesse im eigenen Tätigkeitsgebiet und Arbeitsalltag umgesetzt werden; er oder sie hält die Pflichten gemäss der vorliegenden ICT-Nutzungsweisung ein. Die Mitarbeiterin oder der Mitarbeiter wendet sich mit datenschutzrechtlichen Anliegen und Fragen betreffend die Informationssicherheit an die Ansprechperson für Datenschutzfragen bzw. für Informationssicherheit (falls vorhanden).

Datensicherheit am Arbeitsplatz

Einhaltung geltender Regeln

Generell gilt, dass sich Mitglieder der Kirchenpflege, Mitarbeiterinnen und Mitarbeiter über die geltenden Regeln und Empfehlungen hinsichtlich Datenschutz, Informationssicherheit und der Verwendung von ICT-Mitteln zu informieren haben.

Alle Mitglieder der Kirchenpflege, Mitarbeiterinnen und Mitarbeiter sind für ihr Handeln persönlich verantwortlich, haben bei der Benutzung von ICT-Mitteln achtsam zu handeln und die Privatsphäre anderer Personen stets zu respektieren.

Zwecke

Generell gilt, dass die ICT-Systeme einzig im Kontext der Tätigkeit in der Kirchgemeinde und somit für amtliche und dienstliche Zwecke verwendet werden dürfen. Nicht autorisierte ICT-Mittel dürfen nicht verwendet werden. Eine Verwendung für private Zwecke und während der Arbeitszeit ist nur in Ausnahmefällen und beschränkt auf ein zeitliches Minimum zulässig (siehe § 181 Abs. 1 Vollzugsverordnung der Personalverordnung).

Die Verwendung der ICT-Mittel für private Zwecke, die über Ausnahmefälle hinausgeht, ist grundsätzlich untersagt bzw. ist durch die zuständige Ansprechperson für Datenschutz bzw. für Informationssicherheit (falls vorhanden) zunächst zu prüfen und freizugeben.

Eigentum Kirchgemeinden

Die ICT-Mittel sind Eigentum der Kirchgemeinden. Die Benutzerinnen und Benutzer haben diese mit Sorgfalt zu gebrauchen und mit geeigneten technischen und organisatorischen Massnahmen vor Diebstahl und Beschädigung zu schützen (bspw. Passwort-Schutz, siehe Ziffer 3.3.2 hiervor, Abschliessen von Räumen).

Allfällige Störungen sind der zuständigen Ansprechperson für. Datenschutz bzw. Informationssicherheit (falls vorhanden) umgehend zu melden. Für Supportanfragen sind die in der Kirchgemeinde geltenden Vorgaben und Prozesse zu beachten.

Pflichten bei der Nutzung

Bei der Nutzung der ICT-Systeme haben die Benutzerinnen und Benutzer als Minimalvorgabe die untenstehenden Punkte zu beachten. Für einzelne ICT-Mittel kann die Kirchenpflege zusätzliche Auflagen machen.

- Es sind ausschliesslich die von der Kirchenpflege autorisierte ICT-Systeme zu benutzen und bspw. nur Programme, zu deren Gebrauch die Kirchgemeinde berechtigt ist und eine gültige Lizenz besitzen.
- Es ist sicherzustellen, dass Virenschutzprogramme regelmässig aktualisiert und stets aktiviert sind.
- Generell sind ICT-Systeme (wie Betriebssysteme, Software etc.) stets aktuell zu halten. Updates und Patches müssen regelmässig installiert werden.
- Es ist darauf zu achten, dass regelmässig Sicherheitskopien (*back-ups*) der Daten erstellt werden. Dies geschieht gemäss dem innerhalb der Kirchgemeinde vorgesehen Prozess.
- ICT-Systeme sind gemäss internen Vorgaben und in Absprache mit der Ansprechperson für Informationssicherheit (sofern vorhanden) bzw. Datenschutzfragen zu entsorgen oder reparieren.

Schutz der Zugangsdaten

Benutzerkonten und Meldepflicht

Zugriffe auf ICT-Mittel im Zuge der amtlichen Aufgabenerfüllung sind nur mit von der Kirchgemeinde zur Verfügung gestellten E-Mail-Konten erlaubt. Die Nutzung persönlicher E-Mail-Adressen (z.B. «…@gmail.com» oder «…@bluewin.ch») ist untersagt.

Die Mitglieder der Kirchenpflege, Mitarbeiterinnen und Mitarbeiter haben sämtliche Zugangsdaten für die ICT-Mittel geheim zu halten. Dazu gehören Benutzernamen, Passwörter (s. dazu auch Ziff. 3.2.2 nachfolgend) sowie ggf. weitere Attribute.

Im Falle eines Verlusts oder einem Verdacht auf einen Verlust von Zugangsdaten haben die Betroffenen den Vorfall bei der Ansprechperson für Datenschutz oder Informationssicherheit (falls vorhanden) zu melden.

Passwortschutz

Für den Zugang zu ICT-Mitteln sind stets persönliche Passwörter zu wählen. Dies gilt insbesondere auch dann, wenn von der Kirchgemeinde oder einer Anbieterin/einem Anbieter von ICT-Lösungen ein Initialpasswort zur Verfügung gestellt wird.

Sofern das jeweilige ICT-Mittel erlaubt ist, muss das Passwort mindestens 12 Zeichen lang sein und sowohl Gross-, Kleinbuchstaben, Zahlen und Sonderzeichen (*#!$, etc.) enthalten.

Die Kennwörter sind sodann sicher aufzubewahren. Empfohlen wird die Verwaltung sämtlicher Passwörter in einem sog. Passwort-Manager, der mit einem Masterpasswort gesichert wird (sofern eine Software dafür freigegeben wurde). Alternativ ist die handschriftliche Aufbewahrung der Passwörter an einem sicheren und verschliessbaren Ort empfohlen. Eine Speicherung der Passwörter im Internetbrowser ist untersagt.

Zwei- oder Mehr-Faktor-Authentifizierung

Sofern möglich, ist beim Zugang zu ICT-Mitteln und insbesondere Benutzerkonten eine Zwei- bzw. Mehrfach-Faktor-Authentisierung (2FA, MFA) zu installieren. Dabei werden eine Nutzerin bzw. ein Nutzer eines ICT-Mittels mittels Kombination zweier oder mehrerer Faktoren identifiziert. Beispiele solcher weiteren Komponenten bzw. Faktoren sind Fingerabdrücke oder Transaktionsnummern (TAN).

Clean Desk Policy

Für die Mitglieder der Kirchenpflege, Mitarbeiterinnen und Mitarbeiter gilt eine strikte *Clean Desk Policy*. Unterlagen dürfen weder an den Arbeitsplätzen noch an anderen Orten offen liegen gelassen werden. Auch andere physische Informationsträger wie USB-Sticks, Wechselmedien oder externe Hard Drives sowie mobile Geräte (Laptop, Tablet, Smartphone, etc.) werden nicht unbeaufsichtigt liegen gelassen.

Bei Verlassen des Arbeitsplatzes sperren die Mitglieder der Kirchenpflege, Mitarbeiterinnen und Mitarbeiter stets den Bildschirm (*Clear* Screen *Policy*). Falls man Computer und andere Geräte längere Zeit nicht mehr benötigt oder abwesend ist, so meldet man sich von Systemen ab oder schaltet das Gerät aus.

Bring your own device

Die Mitglieder der Kirchenpflege, Mitarbeiterinnen und Mitarbeiter dürfen private Geräte im Kontext ihrer Tätigkeit bei der Kirchgemeinde nur verwenden, sofern dies ausdrücklich autorisiert wurde. Die Kirchenpflege beschloss am 12.06.2024, dass private Geräte genutzt werden dürfen.

Im Grundsatz ist dabei zu beachten, dass private Daten sowie Daten der Kirchgemeinde strikt getrennt werden und gegenseitige Zugriffe technisch nicht möglich sind.

Weiter gelten bei einem allfälligen Einsatz privater Geräte sämtliche in vorliegender Weisung festgehaltenen Pflichten. Der Kirchenpflege steht es frei, über die Einhaltung dieser Anforderungen einen Nachweis zu verlangen oder zusätzliche Auflagen zu erlassen.

Schutz vor Phishing und Malware

Die Mitglieder der Kirchenpflege, Mitarbeiterinnen und Mitarbeiter müssen geeignete Massnahmen treffen, um sich bzw. die verwendeten ICT-Systeme vor Phishing und Malware zu schützen.

Dafür sind insbesondere folgende Schutzmassnahmen einzuhalten:

- Software zum Schutz vor Malware etc. ist gemäss internen Vorgaben stets zu aktivieren und aktualisieren.
- Verdächtige E-Mails müssen umgehend gelöscht werden und der zuständigen Ansprechperson für Datenschutzfragen oder Informationssicherheit (sofern vorhanden) gemeldet werden.
- Es dürfen keine Unterlagen und Daten an nicht bekannte und verdächtige Absenderadressen gesendet werden sowie keine Anhänge von entsprechenden Absenderadressen geöffnet werden.
- Externe Links oder *Pop-ups* dürfen nur mit gebotener Vorsicht geöffnet und angeklickt werden.
- Fremde Datenträger dürfen ohne Bewilligung nicht an die ICT-Mittel angeschlossen werden.

Arbeiten unterwegs und im Home-Office

Werden ICT-Mittel unterwegs bzw. im Home-Office verwendet, so gelten sämtliche in dieser ICT-Nutzungsrichtlinie enthaltenen Pflichten gleichermassen.

Darüber hinaus ist stets darauf zu achten, dass der Bildschirm vor der Sicht durch Dritte geschützt wird. Dazu muss der Sitzplatz entsprechend gewählt und es muss ein Blickschutzfilter montiert werden.

Gespräche sowie Video-Konferenzen über interne Angelegenheiten und insbesondere sensitive Informationen (bspw. Personendaten oder Amtsgeheimnisse, s. dazu Ziffer 3 bzw. Ziffer 4.5.2 Datenschutz-Handbuch) dürfen nicht in Anwesenheit bzw. in Hörweite Dritter stattfinden.

E-Mail und Internet

E-Mail

Die Mitglieder der Kirchenpflege, Mitarbeiterinnen und Mitarbeiter erhalten einen eigenen E-Mail-Account und eine entsprechende E-Mail-Adresse für ihre Tätigkeit innerhalb der Kirchgemeinde.

Die E-Mail-Adresse ist im Grundsatz lediglich im Kontext der amtlichen Tätigkeit und für entsprechende Korrespondenz zu verwenden. Eine automatische Weiterleitung an andere E-Mail-Accounts ist ohne Bewilligung untersagt.

Die Ablage amtlicher E-Mails im Internet oder auf Datenträgern zu privaten Zwecken ist untersagt.

Die Verwendung des internen Netzwerks ist nur für amtliche Zwecke erlaubt. Insbesondere sind folgende Vorschriften einzuhalten:

- Der Besuch oder die Nutzung von Internetseiten oder elektronischen Kommunikationsplattformen mit rechtswidrigem, pornografischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt sind verboten. Ebenso wenig dürfen entsprechende Inhalte weiterverbreitet werden (siehe § 180 Abs 1 lit. a und b Vollzugsverordnung der Personalverordnung).
- Es dürfen keine elektronischen Kettenbriefe versandt werden (siehe § 180 Abs. 1 lit. c Vollzugsverordnung der Personalverordnung).
- Das Herunterladen oder Installieren von Spielen und Audio- und Videodateien zu privaten Zwecken ist untersagt (siehe § 181 Abs. 2 lit. c Vollzugsverordnung der Personalverordnung).
- Das Abrufen von Internetseiten im Darknet ist untersagt.
- Das Abrufen von Webseiten ohne SSL-Zertifikat (HTTPS) ist möglichst zu vermeiden.

Die Kirchenpflege kann Internetseiten und Kommunikationsplattformen mit unerlaubten Inhalten (siehe Bulletpoint 1 hiervor) sperren (siehe § 180 Abs. 2 und 3 Vollzugsverordnung der Personalverordnung).

Social Media und Cloud Computing

Social Media sowie auf Cloud gehostete Applikationen dürfen nur verwendet werden, sofern sie mit der vorliegenden ICT-Weisung im Einklang stehen. Für die Verwendung von Cloud-Applikationen ist sodann das Datenschutz-Handbuch zu beachten (siehe insbesondere Ziffer 4.3 ff.).

Social Media-Anwendungen dürfen im Rahmen der amtlichen Tätigkeit nur ausnahmsweise und zeitlich beschränkt verwendet werden.

Geheimhaltung und Datenklassifizierung

Schutz von Informationen

Mitglieder der Kirchenpflege, Mitarbeiterinnen und Mitarbeiter unterstehen im Kontext der Tätigkeit für die Kirchgemeinde dem Amtsgeheimnis sowie den anwendbaren Datenschutzgesetzen. Dafür sind die im Datenschutz-Handbuch festgehaltenen Pflichten zu beachten.

Demgemäss ist mit sämtlichen Daten und im Besonderen mit sensitiven Daten (Personendaten, Amtsgeheimnisse) sorgsam umzugehen und sind Vorsichtsmassnahmen zu ergreifen, damit die Daten nicht offengelegt, entwendet, gelöscht oder verändert werden.

Berechtigungs- und Zugriffskonzepte

Die Mitglieder der Kirchenpflege, Mitarbeiterinnen und Mitarbeiter haben die Berechtigungs- und Zugriffsrechte, die für die jeweiligen ICT-Systeme gelten, zu beachten.

Die Kirchenpflege kann ein separates Berechtigungs- und Zugriffskonzept erlassen.

Datenklassifizierung

Die innerhalb der Kirchgemeinde bearbeiteten Dokumente und Informationsbestände unterliegen einer Klassifizierung, wobei sich die Klassen an der jeweiligen Sensitivität und dem Schutzbedarf der jeweiligen Informationen orientiert.

Die Schutzstufe bringt zum Ausdruck, welche technischen und organisatorischen Massnahmen zum Schutz dieser Informationen zwecks Verhinderung unberechtigter Einsicht, Veränderung, Verlust oder Beschädigung zu treffen sind.

Verantwortlich dafür, dass die entsprechenden Informationen klassifiziert werden, ist diejenige Person, die das Dokument erstellt oder verwaltet. Innerhalb der Kirchgemeinde sind folgende Datenklassen massgeblich (siehe dazu auch Datenschutz-Handbuch Ziffer 7.1):

- Öffentlich: Öffentliche Informationen, sind Informationen auf die jeder – innerhalb und ausserhalb der Kirchgemeinde - zugreifen kann und die nicht geschützt sind.
- Intern: Als interne Informationen gelten Informationen, an welchen die Kirchgemeinde, deren Mitglieder, Dritte und/oder Mitglieder der Kirchenpflege, Mitarbeiterinnen und Mitarbeiter ein Interesse haben, dass sie Personen ausserhalb der Institution nicht zur Kenntnis gelangen. Eine Kenntnisnahme durch aussenstehende Dritte würde für sie einen Nachteil aber keine Verletzung einer Schweigepflicht (Geschäfts- oder Amtsgeheimnis) darstellen.
- Vertraulich: Als vertraulich zu klassifizieren sind Informationen, deren Kenntnisnahme durch Unberechtigte den Interessen der Kirchgemeinde, deren Mitgliedern, Dritten oder Mitarbeitenden einen Schaden zufügen kann.
- Geheim: Als geheim werden Informationen klassifiziert, deren Kenntnisnahme durch Unberechtigte den Interessen der Kirchgemeinde, deren Mitgliedern, Dritten oder Mitarbeitenden einen schweren Schaden zufügen kann.

[Sofern die Kirchgemeinde über eine eigene Datenklassifizierung verfügt, kann diese unter Ziffer 4.3 eingefügt werden bzw. es ist hier darauf zu verweisen.]

Bekanntgabe von Informationen

Informationen der Kirchgemeinde, die nicht als öffentlich klassifiziert sind, dürfen nur gestützt auf eine Rechtsgrundlage und in Einklang mit den gesetzlichen Vorschriften gemäss § 16 ff. IDG an Dritte bekannt gegeben werden (siehe zur Definition auch Ziffer 5.3.8 Datenschutz-Handbuch).

Weitere Bestimmungen

Datenschutz-Handbuch

Im Zusammenhang mit der Bearbeitung von Personendaten sowie von Amtsgeheimnissen haben sämtliche Mitglieder der Kirchenpflege, Mitarbeiterinnen und Mitarbeiter die Bestimmungen des Datenschutz-Handbuchs zu befolgen, das auch Pflichten hinsichtlich der Datensicherheit dieser Informationsbestände enthält.

Das Datenschutz-Handbuch ist unter anderem im Zusammenhang mit der Beschaffung von ICT-Systemen, wie dem Erwerb von Software, zu beachten (siehe Ziffer 4.2 ff. betreffend Auftragsdatenbearbeitung und Datenübermittlung ins Ausland).

Meldung von Informationssicherheitsvorfällen

Informationssicherheitsvorfälle liegen vor, wenn Informationen und Datenbestände verloren gehen, unberechtigterweise offengelegt werden oder deren Integrität verletzt wird.

Da die Meldung von Datensicherheitsvorfällen gemäss Datenschutz-Handbuch für sämtliche Informationsbestände (nicht nur Personendaten) gilt, sind die entsprechenden Pflichten auch vorliegend anwendbar (siehe Ziffer 5.4 des Datenschutz-Handbuchs).

Die Meldung hat an die Ansprechperson für Datenschutzfragen bzw. für Informationssicherheit (falls vorhanden) zu erfolgen. Wichtig ist, dass die Meldung von Vorfällen unverzüglich zu erfolgen hat und dem Tagesgeschäft immer vorgeht!

Weitere interne Weisungen

- *Datenschutz-Erklärung*
- *Merkblatt Datenschutz*

Schlussbestimmungen

Folgen bei Beendigung des Arbeitsverhältnisses

Bei Beendigung der amtlichen oder dienstlichen Tätigkeit müssen alle diesbezüglich relevanten Informationen im persönlichen E-Mail-Postfach an die zuständige Person innerhalb der Kirchgemeinde übergeben und allfällige private E-Mails aus dem Postfach gelöscht werden.

Vor dem Austritt sind alle ICT-Mittel entgegen zurückzugeben, soweit nicht etwas anderes vereinbart ist. Sensitive Daten und Unterlagen (wie Kundendaten, Zugangsdaten, etc.) dürfen nicht auf eigenen Systemen gespeichert und weiterhin für private Zwecke verwendet werden.

Sanktionen

Verstösse gegen diese Weisung und die sonstigen Weisungen bezüglich der Anwendung der Informationstechnik und des Umgangs mit personenbezogenen oder anderen schutzwürdigen Daten können personalarbeitsrechtliche und strafrechtliche Konsequenzen haben.

Die personalrechtlichen Konsequenzen richten sich nach der Personalverordnung der Evangelisch-reformierten Landeskirche des Kantons Zürich und der Vollzugsverordnung zur Personalverordnung (s. dazu insbesondere §§ 184 ff. der Vollzugsverordnung).

Gültigkeit

Diese Weisung wurde am […] von der Kirchenpflege verfügt und wird den Mitgliedern der Kirchenpflege, Mitarbeiterinnen und Mitarbeitern auf geeignete Weise bekannt gegeben.

Sie bestätigen schriftlich, über die vorliegende Weisung und die möglichen Konsequenzen aufmerksam gemacht worden zu sein. Die Bestätigung wird im Personaldossier abgelegt.

Diese Weisung tritt am 12.06.2024 in Kraft.