Katholische Kirchgemeinde
Region Rorschach

Reglement über den Einsatz von Informatikmitteln in der Katholischen Kirchgemeinde Region Rorschach (Informatikreglement)

vom 20. September 2022
in Vollzug ab 1. November 2022

Inhaltsverzeichnis

Gestützt auf Art. 15 Abs. 1 lit. j) der Gemeindeordnung vom 1. Januar 2016 (Stand 21. März 2021) erlässt der Kirchenverwaltungsrat folgendes Reglement:

I. Allgemeine Bestimmungen

Art. 1

Zweck

Dieses Reglement regelt das Verhalten im Umgang mit Informatik- und Kommunikationsmitteln der Katholischen Kirchgemeinde Region Rorschach (nachfolgend KKRR). Die Vorgaben dienen dem sicheren sowie wirtschaftlichen Einsatz der Mittel, dem Schutz der damit verwalteten Informationsbestände sowie dem Persönlichkeitsschutz der Benutzenden und Betroffenen.

Art. 2

Geltungsbereich

Das Reglement ist für alle Mitarbeitenden der Katholischen Kirchgemeinde Region Rorschach und Dritte, die Informatik- und Kommunikationsmittel der KKRR einsetzen, verbindlich. Es gilt folglich auch für alle externen informatikrelevanten Vertragspartner der KKRR.

Art. 3

Verantwortlichkeiten

Der Kirchenverwaltungsrat bezeichnet mindestens einen Informationssicherheitsverantwortlichen. Dieser ist für das Umsetzen des vorliegenden Reglements verantwortlich und ist Ansprechperson für Fragen sowie für sicherheitsrelevante Vorkommnisse. Er ist befugt, das Einhalten dieses Reglements zu überprüfen, den Benutzenden Weisungen bezüglich Informationssicherheit zu erteilen und Sanktionen zuhanden der jeweils vorgesetzten Stellen vorzuschlagen.

Art. 4

Der oder die Informationssicherheitsverantwortliche entscheidet über Ausnahmen vom vorliegenden Reglement und die allfälligen kompensierenden Massnahmen/Auflagen. Entsprechende Gesuche sind ihm schriftlich und mit Begründung einzureichen. Über bewilligte Ausnahmen und Auflagen wird Buch geführt.

II. Grundsätze zur Nutzung der Informatikmittel

Art. 5

Eigenverantwortung

Wer Informatik- sowie Kommunikationsmittel verwendet ist für den rechts- und zweckmässigen Einsatz dieser Mittel verantwortlich. Diese Verantwortlichkeit umfasst zudem den Schutz der Personen- und Kundendaten sowie der System- und Organisationsdaten.

Art. 6

Social Media

Soziale Netzwerke wie beispielsweise Facebook, YouTube, Twitter, Instagram, TikTok und LinkedIn dürfen für berufliche Zwecke verwendet werden. Der Nutzer ist verantwortlich für eine angepasste Kommunikationsform auf sämtlichen Plattformen. Es ist insbesondere darauf zu achten, dass keine vertraulichen oder persönliche Daten verbreitet werden.

Für die berufliche Nutzung muss ein «Arbeits-Konto» erstellt werden, welches eindeutig als solches kenntlich gemacht wird (E-Mail-Adresse @kkrr.ch benutzen, Büronummer benutzen, Kürzel mit „_kkrr“ anlegen, an den Namen KKRR anhängen, Profilfoto im beruflichen Kontext).

In privaten Konti dürfen keine Freundschaftsanfragen von besonders schutzbedürftigen Gruppen (z.B. Minderjährige, Klienten der Sozialarbeit etc.) angenommen werden.

Bei der Nutzung von sozialen Netzwerken sind die Regeln des Anstandes und des respektvollen Verhaltens zu befolgen.

Art. 7

Verbotene Aktivitäten

Das Verwenden der Informatik- und Kommunikationsmittel im Zusammenhang mit anstössigen oder illegalen Inhalten ist verboten (Ehrverletzung, Pornographie, Rassismus, Gewalt usw.).

Ebenso sind das Beantworten, Verbreiten und Weiterleiten von Bittbriefen, Kettenbriefen aller Art, Werbeschreiben, Warnmitteilungen und diskriminierenden Nachrichten untersagt.

Mehrfachsendungen von Dokumenten der Katholischen Kirchgemeinde Region Rorschach (Flyer etc.) sind nur mit den eigens dafür generierten Adressen erlaubt.

Bei Mehrfachsendungen ist die Adressierung dermassen zu wählen, dass Drittadressen vom Empfänger nicht eingesehen werden können (z.B. BCC in E-Mail-Programmen).

Art. 8

Schutz vor Malware / bösartiger Software

Desktop-PCs und Laptops sind nach Arbeitsschluss in der Regel vollständig herunterzufahren oder in den Energiesparmodus zu versetzen.

Externe oder mobile Datenträger (USB-Sticks, CDs, DVDs etc.) sind nach dem Beenden der Benutzung – spätestens vor einem Neustart des Computers – zu entfernen.

Art. 9

Installation und Wartung

Für die Installation sowie Wartung der Informatik- und Kommunikationsmittel sind ausschliesslich die Informationssicherheitsverantwortlichen der KKRR oder der externe Dienstleister, der die Mittel zur Verfügung stellt, zuständig. Selbständige Änderungen an den Systemeinstellungen sowie das Installieren oder Entfernen von Hard- und Software durch die Benutzer sind untersagt.
Für Reparatur sowie Entsorgung von Informatik- und Kommunikationsmitteln sind ausschliesslich die Informationssicherheitsverantwortlichen zuständig. Sie stellen sicher, dass keine schützenswerten Daten die KKRR verlassen.

Art. 10

Private Nutzung

Die Informatik-Infrastruktur der KKRR ist für den geschäftlichen Gebrauch bzw. die Erfüllung dienstlicher Aufgaben bestimmt. Die Nutzung für private Zwecke wird toleriert, ist aber auf ein Minimum zu beschränken. Sie darf nur erfolgen, wenn die Erfüllung der geschäftlichen Aufgaben nicht beeinträchtigt wird und die Ressourcenbeanspruchung vernachlässigbar ist.

Private Geräte dürfen weder mittels Kabel noch drahtlos an die Informatiksysteme und Kommunikationsnetzwerke der KKRR angeschlossen werden. Davon ausgenommen sind Smartphones und Tablets, die für dienstliche Zwecke eingesetzt werden. Wer private oder organisationsfremde Informatikmittel für dienstliche Zwecke einsetzt, ist für wirksame Schutzmechanismen gegen Malware verantwortlich. Insbesondere ist sicherzustellen, dass die Virenschutzlösung aktuell sowie aktiv ist und das Betriebssystem wie auch die verwendete Anwendung über die aktuellsten Sicherheitsupdates verfügen.

Art. 11

Radio- und Fernsehempfang

Der Empfang von Radio- und Fernsehprogrammen in Betrieben unterliegt der gesetzlichen Melde- und Gebührenpflicht. Es ist den Benutzenden der KKRR deshalb untersagt, mit Informatik- und Kommunikationsmitteln Radio- und Fernsehprogramme zu empfangen. Nutzt eine Person ein privates Empfangsgerät am Arbeitsplatz, so berechtigen die privat entrichteten Gebühren zum Empfang.

Art. 12

Meldepflicht

Wer sicherheitsrelevante Ereignisse feststellt (z.B. Virenbefall, Verlust von Passwörtern, USB-Sticks, Smartphones, Notebook usw.) oder wer einen Verdacht bezüglich eines sicherheitskritischen Vorgangs hat (z.B. Nutzung einer Zugangs- oder Zugriffsberechtigung durch Dritte), meldet dies umgehend den Informationssicherheitsverantwortlichen. In deren Abwesenheit ist der eigene Vorgesetzte zu informieren.

III. Zugangs- und Zugriffsschutz

Art. 13

Physischer Schutz

Zum Vermeiden von Diebstählen und unberechtigten Netzwerkzugängen sind Fenster und Türen beim Verlassen des Arbeitsplatzes soweit möglich zu verriegeln und vorhandene Schliessvorrichtungen zu nutzen. Ferner ist der Arbeitsplatz so aufzuräumen, dass keine mobilen Datenträger (CDs/DVDs, USB-Sticks usw.) und vertrauliche Unterlagen unverschlossen am Arbeitsplatz zurückgelassen werden (clear desk). Werden mobile Datenträger und vertrauliche Unterlagen in einem Fahrzeug aufbewahrt, müssen diese von aussen nicht sichtbar eingeschlossen sein.

Art. 14

Computersperre, Bildschirmschutz

Bei Abwesenheiten (Pause, Besprechungen, Arbeitsschluss) ist das unbefugte Verwenden des Computers durch das Aktivieren der Bildschirmsperre, das Abmelden vom System oder das Herunterfahren des Systems zu verhindern.

Art. 15

Berechtigungsnachweise

Berechtigungsnachweise wie PINs, Passwörter sowie private Schlüssel der persönlichen Zertifikate sind geheim zu halten. Diese dürfen anderen Personen nicht bekannt beziehungsweise zugänglich gemacht werden – auch nicht einem Systemadministrator. Passwörter müssen sicher sein und die Richtlinien des Informatikanbieters einhalten. Sie dürfen nicht in Verbindung zur eigenen Person stehen (z.B. keine Namen, Geburtsdaten, Hobbies, Telefon- und Autonummern).

Zugeteilte Initialpasswörter und bekannt gewordene Passwörter müssen sofort geändert werden. Aktive Passwörter sind regelmässig zu wechseln. Das neue Passwort darf nicht durch eine einfache logische Überlegung aus dem alten abgeleitet werden können. Geschäftliche Passwörter sind verschieden von privaten Passwörtern zu wählen.

IV. Datensicherheit

Art. 16

Grundsätze

Das Erfassen, Speichern, Verarbeiten, Auswerten und Weitergeben personenbezogener Daten haben unter Berücksichtigung des geltenden Datenschutzgesetzes (eidgenössisch, kantonal, kommunal) zu erfolgen.

Der Zugriff auf Personendaten, die nicht zur Aufgabenerfüllung benötigt werden, ist verboten. Besteht die Möglichkeit einer datenschutzkonformen technischen Lösung, beispielsweise durch das Eingrenzen der Zugriffsrechte, so ist diese umzusetzen. Die Benutzenden melden festgestellte, zu weitgehende Berechtigungen unaufgefordert den Informationssicherheitsverantwortlichen. Personendaten dürfen nur bekannt gegeben werden, wenn die Betroffenen damit einverstanden sind oder die gesetzlichen Grundlagen dazu vorhanden sind. Die Datenschutzkonformität gilt auch für die Veröffentlichung von Personendaten im Intranet (oder einer ähnlichen Plattform) und Internet. Vertrauliche sowie organisationsinterne Informationen dürfen nie in der Öffentlichkeit bearbeitet oder besprochen werden. Für Diskussionen, Telefongespräche oder Bildschirmarbeiten ist folglich ein ungestörter bzw. abgetrennter Bereich aufzusuchen.

Art. 17

Datenablage

Sämtliche erstellte bzw. empfangene Daten müssen auf entsprechenden zentralen Laufwerken, beziehungsweise in Datenbanken (momentan Microsoft Teams) der KKRR abgelegt werden, welche mit entsprechenden Zugriffsrechten geschützt sind. Ein Server-Laufwerk (momentan OneDrive) steht für persönliche Daten zur Verfügung.

Auf privaten oder organisationsfremden Informatikmitteln dürfen keine besonders schützenswerten Personendaten oder geheime Daten der KKRR bearbeitet sowie gespeichert werden. Dies auch dann, wenn die Datenübermittlung verschlüsselt erfolgt. Die Benutzenden sind für die korrekte Ablage und Aufbewahrung der von ihnen erstellten sowie empfangenen Daten im Rahmen ihres Aufgabenbereichs selbst verantwortlich. Private Termine und allfällige Einträge mit besonders schützenswerten Personendaten sind zur Wahrung der Vertraulichkeit im Kalender als "Privat" zu kennzeichnen (aktivieren des Schlosssymbols).

Art. 18

Drucken, Scannen

Ausdrucke mit vertraulichen Informationen sind vorzugsweise per «vertraulicher Druck» (mit Passwortschutz) auszudrucken oder sofort aus dem Drucker zu entfernen. Originale sind sofort aus dem Kopierer/Scanner zu entfernen. Liegengelassene Dokumente mit vertraulichen Informationen sind umgehend dem Urheber/Besitzer zurückzubringen oder den Informationssicherheitsverantwortlichen zu übergeben.

Art. 19

Stellvertretende Zugriffe

Um Zugriffskonflikten bzw. Stellvertretungsproblemen vorzubeugen, sind die Daten generell in einem gemeinsamen Ordner (momentan via Microsoft Teams) abzuspeichern. Der stellvertretende Zugriff auf anderweitig abgelegte Daten, sowie Informationen im Kalender, sind mittels Freigaben und Berechtigungen zu gewährleisten, nicht mittels Weitergabe von persönlichen Passwörtern.

Art. 20

Ungeplante Abwesenheiten

Im Falle von ungeplanten Abwesenheiten können die Informatiksicherheitsverantwortlichen die Freigabe von Daten veranlassen, sofern dies technisch möglich ist. Der Zugriff auf persönliche Daten ist nur in Ausnahmefällen erlaubt und muss mit einem dringenden betrieblichen Bedarf begründet sein.

Art. 21

Cloud Computing

Das Benutzen von externen Cloud-Diensten, wie beispielsweise Dropbox, ist nur dann erlaubt, wenn der Datenaustausch mit den offiziellen Diensten der KKRR (z.B. SharePoint) nicht möglich ist. Dabei müssen die Cloud-Dienste den datenschutzrechtlichen Grundlagen der KKRR genügen. Personenbezogene Daten dürfen nicht mit externen Cloud-Diensten geteilt werden.

Art. 22

Sicheres Löschen von Daten

Defekte Datenträger aller Art sind zwecks fachgerechter und sicherer Entsorgung den Informationssicherheitsverantwortlichen zu übergeben. Nicht mehr gebrauchte Dokumente mit vertraulichen Informationen sind eigenhändig mittels Aktenvernichter oder entsprechenden Containern zu entsorgen.
Austretende Behördenmitglieder haben unterschriftlich zu bestätigen, dass alle schützenswerten Informationen, die ihnen zugänglich waren und die ausserhalb der KKRR bearbeitet oder gespeichert wurden, unwiderruflich gelöscht beziehungsweise vernichtet wurden.

V. Schutz in der Datenübermittlung (E-Mail, Internet)

Art. 23

Umgang mit E-Mails

E-Mails mit fragwürdiger Herkunft, verdächtigem Betreff oder unüblichem Inhalt sind sofort und permanent zu löschen. Deren Beilagen und enthaltenen Links dürfen keinesfalls geöffnet werden, auch wenn die E-Mails über bekannte Absender weitergeleitet wurden.

Art. 24

Vertraulichkeit im E-Mail-Verkehr

E-Mails sind auf ihrem Weg zum Bestimmungsort standardmässig nicht vor unberechtigter Einsicht oder Fälschung geschützt. Darum sind E-Mails mit vertraulichem Inhalt, wie persönlichen Angaben oder anderen zu schützenden Geschäftsinformationen zurückhaltend zu versenden. Wann immer möglich ist die interne Datenablage dafür zu verwenden.

Anlagen können verborgene interne Informationen sowie Informationen über die Entstehung eines Dokumentes enthalten. Zudem ist die Editierbarkeit von Office-Dokumenten nicht immer erwünscht oder der Empfänger nicht mit den erforderlichen Kenntnissen ausgerüstet. Dokumente sind daher vorzugsweise als pdf- oder allenfalls rtf-Dateien weiterzugeben. Wird in einem Dokument eine eingescannte Unterschrift verwendet ist einzig ein Versand als pdf zulässig.

Es ist untersagt interne Adressverzeichnisse an Dritte weiterzuleiten.

Personendaten

Es dürfen keine privaten Kontaktdaten (Adressen, Telefonnummern, E-Mail-Adressen etc.) herausgegeben werden.

In sozialen Netzwerken, Apps etc. dürfen keine beruflichen Kontaktdaten hochgeladen werden (Achtung bei Neu-Installation), weil es sich um persönliche Daten der betroffenen Personen handelt.

Verwendung von Bildern und Fotos

Bei der Nutzung von Bildern aus dem Internet sind die Urheber- und Persönlichkeitsrechte zu beachten.

Fotos von Personen dürfen nur nach schriftlicher Einwilligung veröffentlicht oder weitergeleitet werden. Fotos von Personengruppen mit 20 oder mehr Personen, die an öffentlichen Anlässen gemacht wurden, dürfen veröffentlicht werden.

Art. 25

Neue Kommunikationswege

Die in diesem Kapitel erwähnten Schutzmassnahmen gelten sinngemäss für jegliche neuen und zukünftigen Arten der Kommunikation.

VI. Kollaboration

Art. 26

Kalender

Der seitens KKRR benutzte Kalender (aktuell Outlook) ist grundsätzlich allen Benutzern freizuschalten.
Alle Mitarbeitenden mit einem fixen Pensum von 40% oder mehr, die durch die Kirchgemeinde mit Hardware (z.B. Laptop) ausgestattet sind, müssen geschäftliche Termine in den persönlichen Kalender eintragen und aktuell halten. Private Termine können als privat eingetragen werden.

Art. 27

Telefonie

Die Telefonie der KKRR wird digital zur Verfügung gestellt (momentan via Microsoft Teams). Jeder Nutzer hat eine eigene Nummer. Diese ist über ein privates Mobilgerät ebenfalls abzurufen. Für die Bereitstellung des Mobilgerätes ist der Mitarbeitende persönlich verantwortlich, ebenso für den Unterhalt des Gerätes. Der Kirchenverwaltungsrat entschädigt die Benutzung und den Unterhalt des persönlichen Geräts mit einer jährlichen Pauschale (Bring your own device).
Private Mobiltelefonnummern werden im Zusammenhang mit Aufgaben für die KKRR nicht mehr publiziert.

Nachrichtendienste

Art. 28

Nachrichtendienste wie z.B. Whatsapp können mit der persönlichen Festnetznummer eingerichtet werden. Für betriebliche Kommunikation (intern und extern) ist ausschliesslich diese Variante zu verwenden.

Hinweis: Auf einem Handy können sowohl WhatsApp als auch «WhatsApp for Business» installiert werden, um es gleichzeitig mit zwei Nummern zu benutzen.

Abwesenheit

Art. 29

Bei Abwesenheiten von mehr als einem Tag während der Woche, ist auf den digitalen Kanälen eine automatische Antwort einzustellen (momentan in Outlook und allenfalls WhatsApp for Business).

VII. Missbrauch, Kontrollen und Sanktionen

Konsequenzen

Art. 30

Verstösse gegen dieses Reglement stellen Dienstpflichtverletzungen dar und können personalrechtliche Massnahmen und Schadenersatzansprüche zur Folge haben. Bei strafbaren Handlungen wird gegen die fehlbaren Personen Anzeige erstattet.

Personenbezogene Auswertung der Protokolldaten

Art. 31

Eine personenbezogene Auswertung der Protokolldaten kann in folgenden Fällen erfolgen:

- wenn aufgrund von anonymen Auswertungen Verstösse gegen die vorliegende Weisung festgestellt werden. In diesem Fall werden sämtliche

Benutzende informiert, dass die Auswertung für einen begrenzten Zeitraum personenbezogen erfolgt. Diese Auswertung erfolgt durch den Informatikanbieter unter der Leitung des Informationssicherheitsverantwortlichen.
- wenn der Informationssicherheitsverantwortliche einen Missbrauch feststellt oder vermutet. In diesem Fall beauftragt er die Informatik zur personenbezogenen Auswertung der Protokolldaten. Die betroffene Person muss schriftlich bestätigen, vom Auftrag Kenntnis genommen zu haben.
- wenn sich ein sicherheitsrelevanter Vorfall ereignet hat (bzw. wenn konkrete Anhaltspunkte für einen bevorstehenden Vorfall vorhanden sind), der auf einem Missbrauch beruht. In diesem Fall darf die Informatik ohne Vorwarnung Verbindungsdaten mit personenbezogenen Daten aufzeichnen. Eine personenbezogene Auswertung der Daten darf jedoch erst nach einem Auftrag durch den Informationssicherheitsverantwortlichen und der schriftlichen Bestätigung der betroffenen Personen, vom Auftrag Kenntnis genommen zu haben, erfolgen.
- auf Verlangen des Benutzers selbst oder in Absprache mit ihm, wenn Fehler analysiert und Massnahmen zur Problemlösung entwickelt werden sollen.

VIII. Schlussbestimmungen

Art. 32

Schriftliche Erklärung

Alle Mitarbeitenden und Behördenmitglieder, die Zugang zu den Informatikmitteln, die eine E-Mail-Adresse der Kirchgemeinde und/oder dem Telefonsystem der KKRR haben, unterzeichnen eine Erklärung, mit der sie bestätigen, dass sie auf die vorliegenden Richtlinien aufmerksam gemacht worden sind. Die Erklärung wird im Personaldossier abgelegt.

Art. 33

Vollzugsbeginn

Dieses Reglement tritt per 1. November 2022 in Kraft.

Rorschach, 22. September 2022

NAMENS DES KIRCHENVERWALTUNGSRATES

Pius Riedener	Stefan Meier
Präsident	Aktuar