

Reglement über den Einsatz der Informatikmittel in der Römisch-katholischen Körperschaft des Kantons Zürich (ICT-Reglement)

(vom 7. Juli 2025)¹

Der Synodalrat,

gestützt auf Art. 7 der Kirchenordnung (KO)³, § 7 des Gesetzes über die Information und den Datenschutz (IDG)² sowie §§ 39 und 60 der Anstellungsordnung (AO)⁴,

beschliesst folgendes Reglement:

I Grundlagen

§ 1. Dieses Reglement regelt:

Gegenstand
und Zweck

- a. die Nutzungsbedingungen für den Einsatz der Informatikmittel der Körperschaft,
- b. die Organisation und Verantwortung innerhalb der Körperschaft für den gesetzeskonformen Betrieb und die Nutzung von Informatikmitteln der Körperschaft,
- c. die Überwachung der Informatikmittel der Körperschaft zur Verhinderung von Missbrauch, zur Gewährleistung des sicheren Betriebs und zur Ressourcenplanung,
- d. die Massnahmen zur Gewährleistung der IT-Sicherheit,
- e. die Nutzung von Künstlicher Intelligenz (KI),
- f. die Massnahmen und das Verfahren im Falle von Missbrauch von Informatikmitteln der Körperschaft,
- g. die anonymisierten Auswertungen und die Bearbeitung von personenbezogenen Daten im Rahmen der Überwachung von Informatikmitteln der Körperschaft oder bei Verdacht auf Nichteinhaltung dieses Reglements.

§ 2. ¹ Dieses Reglement sowie die dazugehörigen Anhänge sind für alle Mitarbeitenden und Mitglieder der Römisch-katholischen Körperschaft des Kantons Zürich verbindlich.

Geltungsbereich

² Für Dritte, welche die Informatikmittel der Körperschaft nutzen, wird dieses Reglement auf vertraglicher Basis für verbindlich erklärt. Zuständig ist die Generalsekretärin oder der Generalsekretär.

II Nutzungsvorschriften

Einsatz von Informatikmitteln und Installation von Software

§ 3. ¹ Die geschäftlich anfallenden Daten sind mit der von der Körperschaft zur Verfügung gestellten Hard- und Software zu bearbeiten. Vorbehalten bleiben § 7 Abs. 1 und 2 sowie § 8.

² Die Installation von Hard- und Software sowie Kommunikationseinrichtungen erfolgt ausschliesslich durch die ICT-Verantwortlichen der Körperschaft.

³ Zusätzliche Datensicherungen oder Kopien auf externen Festplatten und USB-Sticks sind verboten.

⁴ Nicht ausdrücklich zugelassene Plattformen und Collaboration Tools sowie Cloud-Dienste sind verboten.

Passwörter und Benutzerberechtigungen

§ 4. ¹ Das Passwort ist persönlich und darf nicht weitergegeben werden.

² Passwörter müssen aus mindestens zehn Stellen bestehen und sollen eine Kombination von Klein- und Grossbuchstaben, Ziffern und Sonderzeichen enthalten. Leicht zu erratende Passwörter und solche, die einen Bezug zur eigenen Person aufweisen (z.B. Name, Name von Angehörigen, Geburtsdatum usw.), sind nicht erlaubt. Geschäftlich genutzte Passwörter dürfen nicht privat verwendet werden.

³ Passwörter sollten regelmässig gewechselt werden. Sie sind sofort zu ändern, wenn ein Verdacht besteht, dass sie Dritten zur Kenntnis gelangt sind. Ein früher bereits benutztes Passwort darf nicht erneut verwendet werden.

⁴ Die Mitarbeitenden dürfen nur ihre persönlichen Benutzerkennungen oder die ihnen zugeteilten funktionellen Kennungen verwenden. Sie sind für die mit ihren Kennungen erfolgten Zugriffe verantwortlich. Der Zugriff auf Daten, die nicht zur Aufgabenerfüllung benötigt werden, ist verboten.

Sicherheitsmassnahmen

§ 5. ¹ Beim Verlassen des Arbeitsplatzes ist die Arbeitsstation zu sperren oder die Benutzerin oder der Benutzer meldet sich vom System ab. Laptops und Smartphones sind entsprechend zu sichern, schutzbedürftige Unterlagen vor Zugang zu schützen.

² Es ist dafür zu sorgen, dass keine Unbefugten Zutritt zu den Arbeitsräumlichkeiten haben. Halten sich Unbefugte in den Büroräumlichkeiten auf, sind Massnahmen zu treffen, die ihnen einen Zugang zu Informationen verwehren.

³ USB-Sticks und externe Festplatten von Dritten sind vor dem Öffnen durch den auf den Informatikmitteln des Synodalrates installierten Virenschutz zu überprüfen. Es dürfen nur Datenträger aus bekannten Quellen verwendet werden.

⁴ Die Mitarbeitenden dürfen die Sicherheitssoftware (Virenschutz, Firewall usw.) nicht ausschalten, blockieren oder deren Konfiguration verändern. E-Mails mit unbekannter Absenderadresse, verdächtigem Betreff oder unüblichem Inhalt sind vorsichtig zu behandeln, da sie von der Virenschutzsoftware nicht erkannte Viren enthalten könnten. Ihre Anhänge sowie Links auf Webseiten sollen keinesfalls geöffnet werden.

§ 6. ¹ Verlorene oder gestohlene Informatikmittel der Körperschaft sind unverzüglich dem Bereich ICT zu melden. Dieser entscheidet über weitere Massnahmen. Meldepflicht

² Bei Verdacht auf Schwachstellen und mögliche IT-Sicherheitsvorfälle (z.B. Virenbefall, Datensicherheit) ist der Bereich ICT zwingend zu informieren. Im Übrigen sind alle beobachteten oder vermuteten IT-Notfälle und Informationssicherheitsvorfälle unverzüglich dem Bereich ICT zu melden.

§ 7. ¹ Personendaten und vertrauliche Sachdaten dürfen mit Ausnahme der eigenen Personendaten nur innerhalb des körperschaftseigenen Netzwerks oder der von der Körperschaft bewilligten Cloud aufbewahrt werden. Personendaten
und vertrauliche
Sachdaten

² Ausgenommen von Abs. 1 sind Personendaten und vertrauliche Sachdaten von Spitalseelsorgenden, welche die spitaleigene Infrastruktur für ihre Tätigkeit benutzen müssen.

³ Personendaten und vertrauliche Sachdaten dürfen online (Internet, soziale Medien, unverschlüsselte E-Mails oder sonstige unverschlüsselten Kommunikationsmittel) nicht genannt werden.

§ 8. ¹ Werden private Smartphones und Tablets zu geschäftlichen Zwecken genutzt, müssen sie mit sechsstelligem Passwort, Fingerprint oder Gesichtserkennung gesichert werden. PCs und Laptops müssen mit mindestens zehnstelligem Passwort geschützt werden. Die Geräte dürfen nicht unbeaufsichtigt gelassen oder Dritten zur Nutzung überlassen werden. Verwendung
von privaten
Geräten zu
geschäftlichen
Zwecken

² Der Zugriff auf geschäftliche Daten sowie deren Verarbeitung darf ausschliesslich über browserbasierte Webanwendungen (z.B. Outlook Webaccess, iKath, onegovGEVER) erfolgen.

³ Das Herunterladen oder Speichern von geschäftlichen Daten auf private Geräte ist mit Ausnahme der eigenen Personendaten nicht zulässig.

Private Nutzung
der Informatik-
mittel und der
Infrastruktur
der Körperschaft

§ 9. ¹ Die private nicht kommerzielle Nutzung der IT-Infrastruktur der Körperschaft ist erlaubt. Sie ist jedoch während der Arbeitszeit auf ein Minimum zu beschränken und sollte grundsätzlich nur während Pausen erfolgen.

² Das Herunterladen von privaten Dateien in grosser Menge oder mit grosser Netzwerkbelastung sowie deren Speicherung in der Datenablage (Foto-, Video- und Musikdateien) sind nicht erlaubt.

³ Der Zugang zum Internet mit privaten Geräten ist nur im Gäste- oder Mitarbeitendenbereich des WLAN erlaubt.

Private E-Mails
und Weiter-
leitung von
E-Mails

§ 10. ¹ Das Versenden und Empfangen privater E-Mails über das Mail-Konto der Körperschaft ist erlaubt. Entsprechende E-Mails müssen in einem als «privat» bezeichneten Ordner abgelegt werden. Bei der automatischen Sicherung (Backup) der E-Mails der Arbeitnehmenden werden auch die privaten E-Mails gesichert.

² Private E-Mails, welche nicht als solche gekennzeichnet sind, gelten als geschäftliche E-Mails.

³ Nicht erlaubt ist das Publizieren der dienstlichen E-Mail-Adresse auf Webseiten zu privaten Zwecken.

⁴ Das automatische Weiterleiten (Forwarding) von E-Mails an die private sowie weitere interne und externe E-Mail-Adressen ist verboten. Bei mehrtägiger Abwesenheit ist im E-Mail-Konto eine entsprechende Abwesenheitsnotiz zu erstellen.

Nutzung von
Künstlicher
Intelligenz (KI)

§ 11. ¹ Die Mitarbeitenden und Mitglieder der Körperschaft dürfen bei ihrer geschäftlichen Tätigkeit Technologien und Systeme nutzen, die auf Künstlicher Intelligenz basieren (KI-basierte Technologien und Systeme oder kurz: KI).

² Um einen ethischen, rechtskonformen und sicheren Einsatz von KI-basierten Technologien und Systemen zu gewährleisten, gelten die folgenden Vorgaben:

- a. der Einsatz von KI-basierten Technologien und Systemen muss durch den Bereich ICT genehmigt werden. Die zugelassenen KI-Systeme werden in einem Anhang zu diesem Reglement festgelegt. Nicht zugelassene KI-basierte Technologien und Systeme sind verboten,
- b. KI darf nur für Zwecke eingesetzt werden, die dem Geschäftszweck der Körperschaft entsprechen und rechtskonform sind,

- c. der Einsatz von KI darf nicht zu Diskriminierung («Bias»), Verletzung des Datenschutzes oder unethischen, rechtswidrigen oder strafbaren Handlungen führen,
- d. die Ergebnisse aus der KI-Nutzung dürfen nicht unvoreingenommen und ohne menschliches Monitoring übernommen werden (Plausibilitätskontrolle),
- e. bei der Nutzung von KI-Systemen dürfen Personendaten, einschliesslich besonderer Personendaten, sowie vertrauliche Sachdaten der Körperschaft nur im Rahmen der kirchlichen Aufgabenerfüllung und in vom Bereich ICT bewilligten geschlossenen KI-Systemen (keine Open Source AI) verwendet werden; die Datensicherheit ist stets zu gewährleisten,
- f. werden besondere Personendaten in KI-Systemen bearbeitet, ist vorab eine datenschutzrechtliche Risikoabwägung des entsprechenden KI-Systems durch die Beauftragte oder den Beauftragten für den Datenschutz vorzunehmen. Ergibt sich daraus ein hohes Risiko für die betroffenen Personen, ist eine Datenschutz-Folgenabschätzung gemäss den geltenden datenschutzrechtlichen Vorgaben durchzuführen. Ist die Bearbeitung und Verwendung von besonderen Personendaten rechtlich notwendig, sind angemessene datenschutzrechtliche Schutzmassnahmen wie Anonymisierung oder Pseudonymisierung zu treffen,
- g. der Einsatz von KI muss für Betroffene transparent sein; bei der Verwendung von KI in Arbeitsergebnissen ist entsprechend darauf hinzuweisen,
- h. sofern Entscheidungen auf Basis von KI getroffen werden, ist dieser Prozess nachvollziehbar zu dokumentieren,
- i. KI darf nicht für automatisierte Entscheidungen verwendet werden, die für die Betroffenen erhebliche rechtliche oder ethische Konsequenzen haben können.

³ Weiterführende Vorgaben und konkrete Anwendungsrichtlinien können in einem gesonderten Merkblatt festgelegt werden.

⁴ Der Bereich ICT kann die Einhaltung der Vorgaben zur KI-Nutzung eigenständig überprüfen und bei Bedarf oder missbräuchlicher Verwendung die Nutzung einschränken oder verbieten.

§ 12. ¹ Der Zugang zu geschäftlichen Daten bei Abwesenheiten darf grundsätzlich nur mit Zustimmung der betreffenden Mitarbeiterin oder des betreffenden Mitarbeiters erfolgen.

Zugang zu
geschäftlichen
Daten bei
Abwesenheiten

² Sofern betrieblich notwendig, ist die Bereichsleiterin oder der Bereichsleiter Personal bei längerer Abwesenheit (aufgrund von Unfall, Krankheit oder sonstigen ausserordentlichen Ereignissen) einer oder eines Mitarbeitenden nach mehrmalig versuchter Rücksprache mit der

oder dem Mitarbeitenden berechtigt, auf deren oder dessen geschäftliche Daten (persönliches Laufwerk, Datenablage und E-Mail-Konto) zuzugreifen. Sie oder er macht es mit Zustimmung und unter Mitwirkung der oder des Beauftragten für den Datenschutz.

³ Die als privat gekennzeichneten Daten bleiben in der Datenablage der betroffenen Person. Die Vertraulichkeit und der Schutz der nicht als privat gekennzeichneten Daten kann nicht gewährleistet werden.

⁴ Der Zugang und die Datenverarbeitung werden genau festgehalten und protokolliert.

Rechtswidrige
Nutzung

§ 13. Dokumente, Videos und Bilder sowie E-Mails, Webseiten und andere Webinhalte mit rassistischen, pornografischen, sexistischen, gewaltverherrlichenden oder rechtswidrigen Inhalten dürfen weder konsumiert noch heruntergeladen oder weiterverbreitet werden.

III Organisation und Verantwortung

Synodalrat

§ 14. Der Synodalrat ist verantwortlich für den Betrieb der körperschaftseigenen IT-Infrastruktur. Er gewährleistet die rechtskonforme Nutzung, die Datensicherheit sowie den Daten- und Persönlichkeitsschutz der Angestellten und Behördenmitglieder der Körperschaft.

Bereich ICT

§ 15. ¹ Der Bereich ICT ist verantwortlich für die Erstellung der IT-Konzepte der Körperschaft, deren Umsetzung und Überwachung. Er trifft die notwendigen technischen Massnahmen zur Gewährleistung der Datensicherheit und des Datenschutzes.

² Er ist insbesondere zuständig für:

- a. die Installation von Software und Programmen gemäss § 3,
- b. das Sperren und Freischalten von Internetseiten sowie sozialer Medien und Plattformen,
- c. die Anordnung und Umsetzung von angemessenen technischen Massnahmen, wie z.B. Firewalls, Spamfilter, Virenschutz usw.,
- d. die Löschung von als Spam erkannten Daten,
- e. die technische Behebung von Verstössen gegen Nutzungsvorschriften dieses Reglements, insbesondere das unverzügliche Entfernen von widerrechtlicher oder missbräuchlicher Hard- und Software,
- f. Notfallmassnahmen, welche schnell getroffen werden müssen (z.B. für kompromittierte Dienste),

- g. Massnahmen zur Gewährleistung der IT-Sicherheit gemäss §§ 18 und 19,
- h. Massnahmen gemäss § 21.

§ 16. ¹ Die oder der Beauftragte für den Datenschutz in der Körperschaft ist eine Stelle des Bereichs ICT der Körperschaft.

Beauftragte
oder Beauftrag-
ter für den
Datenschutz
in der Körper-
schaft

² Die oder der Beauftragte für den Datenschutz in der Körperschaft ist die zuständige Ansprechperson in Datenschutzfragen im Sinne von Art. 7 Abs. 1 der Kirchenordnung. Sie oder er ist verantwortlich für die Überprüfung und Überwachung der Datensicherheit und des Datenschutzes der IT-Konzepte und der IT-Infrastruktur der Körperschaft, insbesondere was das Feststellen und Beheben von IT-Sicherheitsmängeln betrifft. Sie oder er schlägt Sicherheitsmassnahmen vor und gibt Sicherheitsempfehlungen ab, um die IT-Anwendungen und -Systeme vor unbefugten Einwirkungen und vor unbefugtem Zugriff zu schützen. Sie kann zur Abklärung und Behebung von Sicherheitsmängeln externe Fachpersonen beiziehen.

³ Die oder der Beauftragte für den Datenschutz ist im Weiteren verantwortlich für:

- a. die Überprüfung der Einhaltung von datenschutzrechtlichen Vorschriften und Richtlinien sowie die Einhaltung der Nutzungsvorschriften dieses Reglements,
- b. Massnahmen gemäss § 21,
- c. die Auswertung der periodischen anonymisierten Berichte gemäss § 19,
- d. die Einleitung des Verfahrens einer personenbezogenen Auswertung sowie die Auswertung der Daten gemäss § 22.

§ 17. ¹ Als Betreiberstellen gelten die Informatikdienste, die für den Betrieb der IT-Infrastruktur und der Dienste der Körperschaft zuständig sind.

Betreiberstelle

² Durch Vertrag des Synodalrates oder Weisung des Bereichs ICT wird sichergestellt, dass die Betreiberstellen die rechtskonforme und sichere Nutzung der IT-Infrastruktur und der Dienste der Körperschaft ermöglichen.

IV Massnahmen zur Gewährleistung der IT-Sicherheit

Technische Schutzvorkehrungen und Nutzungsrichtlinien

§ 18. Der Bereich ICT sorgt dafür, dass die IT-Infrastruktur rechtskonform genutzt wird. Er trifft die dazu nötigen technischen Schutzvorkehrungen, erlässt Nutzungsrichtlinien für Mitarbeitende sowie Drittnutzende und überwacht die Einhaltung dieses Reglements.

Aufzeichnung und Auswertung von Randdaten

§ 19. ¹ Der Bereich ICT zeichnet bestimmte Randdaten auf und wertet diese periodisch anonymisiert aus. Die Randdaten werden für höchstens zwölf Monate aufgezeichnet und beschränken sich auf folgende Informationen:

- a. interner Speicher (Homedrive, Teamfolder, s2Drive),
- b. Telefonie pro Hauptnummer zuhanden der Finanzbuchhaltung zum Zweck der Weiterverrechnung an die Kostenstellen (allgemeine Kosten, kostenpflichtige Telefonnummern und Auslandstelefonie),
- c. Webtraffic (externer Datenfluss), Überwachung von Zieladressen,
- d. Netzwerktraffic (interner Datenfluss) oder Datenvolumen,
- e. letztmalige Systemanmeldungen der PCs und Laptops in der Körperschaft,
- f. Installation von illegaler Software auf der IT-Infrastruktur der Körperschaft.

² Die Auswertungen dürfen keine Rückschlüsse auf einzelne Mitarbeitende zulassen. Insbesondere dürfen sich aus ihnen weder die einzelnen Mitarbeitenden noch die einzelnen Arbeitsplätze ergeben.

³ Besteht aufgrund der anonymisierten Auswertungen ein erheblicher Verdacht auf Missbrauch im Sinne von § 20, erstellt die oder der Beauftragte für den Datenschutz einen Bericht zuhanden der Generalsekretärin oder des Generalsekretärs und leitet damit das Verfahren der personenbezogenen Auswertung gemäss § 22 ein.

V Verfahren und Folgen bei Missbrauch oder erheblichem Verdacht auf Missbrauch

Missbrauch

§ 20. Ein Missbrauch im Sinne dieses Reglements liegt bei einem Verstoß gegen die Nutzungsvorschriften gemäss §§ 3–11 und 13 sowie 15 Abs. 2 vor.

§ 21. ¹ Stellt der Bereich ICT oder die oder der Beauftragte für den Datenschutz im Rahmen ihrer Aufgabenerfüllung Verstösse gegen dieses Reglement fest oder werden dem Bereich ICT oder der oder dem Beauftragten für den Datenschutz solche gemeldet, ergreift die Bereichsleiterin oder der Bereichsleiter ICT insbesondere die folgenden Massnahmen:

Weisungen, Ersatzvornahmen und vorsorgliche Massnahmen

- a. Anweisung an die Mitarbeiterin oder den Mitarbeiter, die missbräuchliche Nutzung innert Frist zu beseitigen und künftig zu unterlassen,
- b. die eigenmächtige Beseitigung des rechtswidrigen Zustands, sofern dieser entgegen der Anweisung nicht innert Frist durch die Mitarbeiterin oder den Mitarbeiter selber erfolgt oder erfolgen kann,
- c. vorsorgliche Sicherung von Daten sowie missbräuchlicher Hard- und Software zu Beweiszwecken bei erheblichem Verdacht auf eine Straftat nach dem Schweizerischen Strafgesetzbuch⁵ nach Rücksprache mit der Generalsekretärin oder dem Generalsekretär sowie der Bereichsleiterin oder dem Bereichsleiter Personal. Wird kein Strafverfahren eingeleitet, wird das gesicherte Beweismaterial vernichtet.

² Der Bereich ICT oder die oder der Beauftragte für den Datenschutz informiert die zuständige Bereichsleiterin oder den zuständigen Bereichsleiter, die linienvorgesetzte Person sowie die Bereichsleiterin oder den Bereichsleiter Personal über die getroffenen Massnahmen.

§ 22. ¹ Gestützt auf den Bericht der anonymisierten Auswertung gemäss § 19 ordnet die Generalsekretärin oder der Generalsekretär eine personenbezogene Auswertung an. Sie oder er informiert die Bereichsleiterin oder den Bereichsleiter Personal vorgängig über die Anordnung.

Verfahren der personenbezogenen Auswertungen

² Die Generalsekretärin oder der Generalsekretär informiert die betroffene Mitarbeiterin oder den betroffenen Mitarbeiter über Inhalt und Dauer der personenbezogenen Auswertung.

³ Die personenbezogenen Auswertungen beziehen sich auf die missbrauchsrelevanten Bereiche der anonymisierten Auswertungen unter Angabe des Namens der oder des Nutzenden.

⁴ Die Betreiberstelle stellt die als vertraulich deklarierten Auswertungen der oder dem Beauftragten für den Datenschutz zu.

⁵ Die Generalsekretärin oder der Generalsekretär entscheidet zusammen mit der Bereichsleiterin oder dem Bereichsleiter Personal aufgrund der personenbezogenen Auswertung, ob der Personalkommission beantragt wird, eine Massnahme gemäss §§ 21 und 23 (weitere Folgen des Missbrauchs) einzuleiten sowie andere Massnahmen zu treffen.

⁶ Die Generalsekretärin oder der Generalsekretär teilt der Mitarbeiterin oder dem Mitarbeiter den Entscheid mit.

⁷ Die Protokolle der personenbezogenen Auswertungen werden spätestens nach zwölf Monaten gelöscht, wenn sich der Verdacht auf Missbrauch nicht bestätigt oder sämtliche Verfahren rechtskräftig abgeschlossen sind. Die betreffende Mitarbeiterin oder der betreffende Mitarbeiter wird über die Löschung informiert.

Weitere Folgen
des Missbrauchs

§ 23. ¹ Bei Missbrauch, wiederholtem Missbrauch im Sinne von § 20 oder Nichtbefolgung der Weisungen des Bereichs ICT sowie der oder des Beauftragten für den Datenschutz werden zudem personalrechtliche Massnahmen nach der Anstellungsordnung geprüft und eingeleitet. Zuständig für den Entscheid über personalrechtliche Massnahmen ist die Personalkommission.

² Vorbehalten bleibt die Einleitung eines Strafverfahrens und die Geltendmachung von Schadenersatzansprüchen durch den Synodalarat. Zuständig ist die Generalsekretärin oder der Generalsekretär.

VI Schlussbestimmungen

Bestätigung der
Kenntnisnahme
des Reglements

§ 24. Jede Mitarbeiterin und jeder Mitarbeiter sowie jedes Mitglied der Körperschaft unterzeichnet das Reglement als Erklärung, dass sie oder er das Reglement gelesen und den Inhalt zur Kenntnis genommen hat.

Inkrafttreten

§ 25. Dieses Reglement tritt am 1. Oktober 2025 in Kraft. Es ersetzt das ICT-Nutzungsreglement vom 20. Mai 2019.

¹ [OS 80.211](#); Begründung siehe [ABI 2025-07-18](#).

² [LS 170.4](#).

³ [LS 182.10](#).

⁴ [LS 182.41](#).

⁵ [SR 311.0](#).