

Reglement über den Betrieb der Informatikmittel durch die Nutzer der Kath. Kirchgemeinde Alpnach

Version 4
September 2026

Integrierender Bestandteil zum Arbeitsvertrag oder Behördenvertrag

Legende:	KGA	Kath. Kirchgemeinde Alpnach
	ISV	Informationssicherheitsverantwortlicher
	Supportstelle	externe IT-Firma, die uns technisch unterstützt

Aus Gründen der besseren Lesbarkeit wird im Reglement ausschliesslich die männliche Form angewendet. Sie bezieht sich auf Personen aller Geschlechter.

Art. 1

Einleitung

¹ Dieses Reglement regelt die Nutzung der Informatikmittel (IT-Mittel), im Speziellen den Gebrauch von E-Mail und Internet sowie die Verwendung mobiler Geräte.

² Weiter wird der verantwortungsvolle Umgang mit Informationen, insbesondere mit Personendaten, thematisiert.

³ Die von der KGA hierfür zur Verfügung gestellte Infrastruktur ist von den Nutzern sorgfältig und gemäss diesem Reglement einzusetzen. Jede missbräuchliche Nutzung ist untersagt.

Art. 2

Geltungsbereich

Dieses Reglement gilt für jegliche Nutzung der durch die KGA zur Verfügung gestellten IT-Infrastruktur oder IT-Infrastrukturdienste. Diese umfassen Hardware (Geräte), Software (Programme), Netzwerke, Daten, Support, etc. Das Reglement gilt auch für jegliche Nutzung privater Geräte, welche über die IT-Infrastruktur oder IT-Dienste der KGA erfolgt.

Art. 3

Begriffe und allgemeine Informationen

In nachfolgender Definition «Nutzer» sind alle Personen eingeschlossen, welche die IT-Dienstleistungen der KGA nutzen.

IT

Kurzbezeichnung für den Begriff Informations- und Kommunikationstechnologie. Darunter fallen jegliche Kommunikationsanwendungen wie Notebooks, Tablets, Smartphones, IP-Telefonie, Hardware und Software für Computer und Netzwerke, Satellitensysteme, sowie für die verschiedenen Dienstleistungen und Anwendungen im Informatikbereich. Die gemachte Aufzählung ist nicht abschliessend und lediglich exemplarisch zu verstehen.

Personendaten

¹ Unter personenbezogenen Daten versteht man alle Daten, die eine bestimmte oder bestimmbare natürliche Person betreffen. Dabei kann es sich um gängige Angaben wie die E-Mail-Adresse, Telefonnummer oder das Bild dieser Person handeln, aber auch um Informationen zu körperlichen, kulturellen oder gesellschaftlichen Merkmalen.

² Bei Unsicherheiten, inwieweit die Rechtsvorschriften einzuhalten sind, haben sich die Mitarbeitenden / Behördenmitglieder an den ISV zur Klärung zu wenden.

Cloud

Die Cloud beschreibt die Bereitstellung von Informatik-Infrastruktur wie beispielsweise Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung über das Internet (zurzeit Office 365 SharePoint und OneDrive, kOOL Verwaltungssoftware, Cloud des Buchhaltungsprogramms).

IT Geräte

Zu mobilen Geräten gehören Laptop, Notebook, Tablet, Smartphone, Bildschirm, USB und sonstige Datenträger.

Externe Daten

Daten, welche von Personen ausserhalb der KGA eingesehen werden können (Beispiel: Homepage usw.).

Messagingdienste

Damit sind alle Text-, Bild- oder Filmnachrichtendienste ausserhalb der MS Office Produkte (Outlook, Teams) gemeint. Messagingdienste sind zum Beispiel Zoom und MSN.

Art. 4

Verantwortung

¹ Die KGA bezeichnet einen Informationssicherheitsverantwortlichen (ISV). Dieser ist für die Einhaltung dieses Reglements verantwortlich und ist Ansprechstelle für Fragen und sicherheitsrelevante Vorkommnisse.

² In Absprache mit der IT-verantwortlichen Person der KGA ist dieser befugt, den Mitarbeitenden Weisungen bezüglich Informationssicherheit zu erteilen.

³ Die Nutzer sind verpflichtet, dieses Reglement sowie weitere gesetzliche Grundlagen und Weisungen (allg. Vorgaben der KGA, Merkblätter etc.) zu beachten. Sie haben die vollständige Kenntnisnahme mit Unterschrift zu bestätigen.

⁴ Die Nutzer sind verpflichtet, die ihnen zur Verfügung gestellten IT-Mittel recht- und zweckmässig einzusetzen und mit den Informationen sorgfältig umzugehen.

⁵ Die Nutzer melden dem ISV alle sicherheitsrelevanten Ereignisse (Probleme, Vorfälle, Mängel usw.) sowie Schäden und/oder Verlust von Hardware, mobilen Geräte und Software.

Art. 5

Datenschutz

¹ Datenschutz dient dem Schutz der Privatsphäre und der Persönlichkeitsrechte. Er dient dem Schutz vor missbräuchlicher Datenbearbeitung. Der technische Datenschutz umfasst alle technischen Massnahmen und Vorkehrungen, um personenbezogene Daten vor unbefugtem Zugriff, Verlust oder Missbrauch zu schützen.

² Die Nutzer beachten bei der Nutzung der IT-Infrastruktur, insbesondere bei der Bearbeitung von Personendaten, die Bestimmungen des eidgenössischen und kantonalen Datenschutzrechts.

³ Ohne Rechtfertigungsgrund betreffender Personen dürfen keine personenbezogenen Daten extern übermittelt oder veröffentlicht werden. Dies betrifft jegliche personenbezogene Daten.

⁴ Die Abbildung einer Gruppe von Menschen auf öffentlichen Plätzen oder Veranstaltungen (Kirchenfeiern usw.), bei der keine Personen besonders hervorgehoben sind, ist zulässig; dafür muss keine Zustimmung der darauf sichtbaren Personen eingeholt werden. Bei allen übrigen Aufnahmen, auf welchen Personen identifizierbar sind, muss das Einverständnis jeder Person mit dem Dokument «Bild und Videoaufnahme» schriftlich eingeholt werden.

⁵ Über die Zugriffsberechtigung zur IT-Infrastruktur entscheidet der Pfarreikoordinator auf Empfehlung des ISV.

⁶ Die Nutzer der IT-Infrastruktur achten darauf, dass keine Unbefugten Zugang zu den IT-Mitteln haben. Halten sich externe Personen in den Räumlichkeiten auf, sind Massnahmen zu treffen, die einen unbefugten Zugang zu Informationen verhindern.

⁷ Ausdrücke mit vertraulichen Informationen sind umgehend aus dem Drucker zu entfernen.

⁸ Der Zugriff auf Personendaten, die nicht zur Aufgabenerfüllung benötigt werden, ist untersagt.

Art. 6

Passwörter und Authentifizierung

Passwörter sind vertraulich zu behandeln. Sie dürfen nicht unverschlüsselt abgelegt, gespeichert oder anderen Personen bekannt gegeben werden.

Art. 7

Datenablage, Datensicherung, Archivierung

¹ Geschäftsbezogene Daten (Daten der Kirchgemeinde und der Pfarrei) müssen auf der Cloud der Kirchgemeinde (Office 365 SharePoint, OneDrive, Verwaltungssoftware kOOL, Cloud des Buchhaltungsprogramms) oder dem Medienspeicher (NAS) gespeichert werden. Für persönliche, private Daten steht nur die Cloud OneDrive zur Verfügung.

² Die Daten auf dem SharePoint und OneDrive der Kirchgemeinde werden gemäss Standardvertrag bei Microsoft für 60 Tage gesichert.

³ Bei lokal installierter Software, bei welcher geschäftliche Daten lokal gespeichert werden, müssen in Rücksprache mit der Supportstelle Massnahmen zur Datensicherung getroffen werden.

Art. 8

Anschaffung IT-Geräte für Personen im Teilzeitpensum

ab 50%:	Laptop wird zu 100% bezahlt oder zur Verfügung gestellt.
bei 40%:	80% bezahlt / zur Verfügung gestellt
bei 30%:	60% bezahlt / zur Verfügung gestellt
bei 20%:	40% bezahlt / zur Verfügung gestellt

¹ Der Laptop wird durch den Mitarbeitenden angeschafft (ev. in Absprache mit dem ISV) und für die Arbeit der Kirchgemeinde genutzt. Die Rechnungsquittung muss der Kirchgemeinde vorgelegt werden. Es werden anteilmässig die Kosten des effektiven Rechnungsbetrages übernommen (siehe Kasten oben).

² Der Maximalbetrag, der übernommen wird, beträgt CHF 1'500.– (inkl. Software). Die Installation wird nicht übernommen.

³ Nutzer in der Probezeit haben kein Anrecht auf die Übernahme der Kosten.

⁴ Bei einem Austritt vor Ablauf eines Jahres müssen die Kosten anteilmässig (50% des von der KGA übernommenen Betrages) zurückbezahlt werden.

⁵ Die Kirchgemeinde übernimmt die Kosten maximum alle 5 Jahre.

⁶ Von dieser Regelung ausgenommen sind feste Arbeitsplätze von Sekretariat und Verwaltung.

Art. 9

Löschung und Entsorgung von Datenträgern

Nicht mehr benötigte Daten müssen von lokalen und mobilen Datenträgern (z.B. USB-Datenträger, Speicherkarten usw.) unwiederbringlich gelöscht werden. Der ISV ist dafür zuständig.

Art. 10

Massnahmen bei Austritt

¹ Das Verfügungsrecht über geschäftliche Informationen auf dem E-Mail-Konto von ausscheidenden Nutzern steht der KGA zu.

² Die Benutzerkonten werden umgehend nach Beendigung des Arbeitsverhältnisses deaktiviert und gemäss Austritts-Checkliste KGA frühestens nach drei Monaten gelöscht.

³ Allfällige private E-Mails und Daten werden nach Beendigung des Arbeitsverhältnisses / der Behördentätigkeit von der IT-Infrastruktur entfernt.

Art. 11

Informationssicherheit

¹ Die Anwender dürfen die Sicherheitssoftware (Virenschutz, Firewall usw.) nicht ausschalten, blockieren oder umkonfigurieren.

² E-Mails mit unbekanntem Absender, verdächtigem Betreff oder unüblichem Inhalt sind im Hinblick darauf, dass sie von der Virenschutzsoftware nicht erkannte Viren enthalten könnten, vorsichtig zu behandeln und im Zweifelsfall zu löschen. Bei Verdacht auf Virenbefall den PC oder das Gerät ausschalten und sofort bei der Supportstelle melden.

³ Bei einem privaten Gerät (PC, Notebook, Tablet usw. gemäss Artikel 8) wird erwartet, dass ein Virenschutz vorhanden und die Software-Updates auf dem neusten Stand sind.

Art. 12

Nutzung von E-Mail

¹ E-Mail und Internet werden für die notwendige Erfüllung dienstlicher Aufgaben nach den Grundsätzen der Wirtschaftlichkeit, der Datensicherheit und des Datenschutzes eingesetzt.

² E-Mails mit vertraulichem Inhalt (z.B. Personendaten) müssen mit besonderer Aufmerksamkeit behandelt werden. Ein E-Mailversand von solchen Daten ist auf das absolute Notwendigste zu reduzieren.

³ Das Freigeben der persönlichen Mailbox an eine Drittperson ist nicht erlaubt. Bei mehrtägiger Abwesenheit sollte die Funktion des Abwesenheitsassistenten genutzt werden.

⁴ Die automatische Umleitung von E-Mails an eine private Mailbox ist untersagt. Das E-Mail-System darf in zurückhaltendem Masse auch für private Zwecke verwendet werden.

⁵ Das Versenden von E-Mails mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt oder mit der Aufforderung zum Weiterversand im Schneeballsystem ist verboten.

⁶ Jede E-Mail wird vor der Zustellung auf SPAM und missbräuchlichen Inhalt durch einen technischen Filter geprüft.

⁷ Irrtümlich in Quarantäne gesetzte E-Mails können weitergeleitet werden. E-Mails in Quarantäne werden nach 180 Tagen automatisch gelöscht und werden nicht gesichert.

Art.13

Internet und Cloud

¹ Die Nutzung von externen Messaging Diensten (siehe Begriffe) sind nur erlaubt, wenn datenschutzrechtliche Belange gewahrt werden.

² Der Zugriff auf Internetseiten mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt ist verboten.

³ Geschäftsrelevante Daten mit schützenswerten Personendaten (Datenschutz) dürfen nur mit der Zustimmung betreffender Personen publiziert werden.

⁴ Die Verteilung und Speicherung von urheberrechtlich geschütztem Material (Musik, Bilder, Filme, Dateien) ist ohne Genehmigung des Herstellers oder Lizenz des Urhebers untersagt.

Art. 14

KI Nutzung

¹ Der Einsatz von KI hat stets im Einklang mit den Unternehmenswerten, geltenden Gesetzen sowie internen Richtlinien zu erfolgen. KI dient der Unterstützung menschlicher Tätigkeiten und ersetzt keine fachliche, rechtliche oder ethische Verantwortung. Entscheidungen mit wesentlichen Auswirkungen dürfen nicht ausschließlich auf KI-Ergebnissen basieren.

² Bei der Nutzung von KI sind potenzielle Risiken wie fehlerhafte Ergebnisse, Verzerrungen (Bias), Datenabfluss oder Manipulation zu berücksichtigen. KI-Ergebnisse sind kritisch zu prüfen und dürfen nicht ungeprüft weiterverwendet oder veröffentlicht werden. KI generierte Unterlagen müssen als solche benannt werden.

³ Die Verantwortung für Inhalte, Entscheidungen und Handlungen, die unter Nutzung von KI erfolgen, liegt stets bei den jeweiligen Mitarbeitenden. Führungskräfte stellen sicher, dass ihre Teams über die zulässige Nutzung von KI informiert und entsprechend geschult sind.

Art. 15

Private Nutzung von IT-Mitteln

Die Benützung von IT-Mitteln der KGA für private Zwecke ist grundsätzlich gestattet, soweit dadurch die Systemsicherheit, Ressourcen wie Speicher und Übertragungskapazität nicht im Übermass belastet werden. Vorsicht ist geboten bei Finanztransaktionen (Telebanking, Börsengeschäft, o. ä.), Online-Spielen (Glücksspiele usw.), Auktionen oder Versteigerungen.

Art. 16

Sicherheit der mobilen Geräte

¹ Für das digitale Arbeiten werden Grundkenntnisse in Microsoft Betriebssysteme und Microsoft Office vorausgesetzt.

² Der Zugang zu Apps, Software und Clouds mit Daten der KGA müssen zwingend passwortgeschützt werden.

³ Im Allgemeinen sind Installationen von Anwendungen (Apps) auf mobilen Apple- und Android-Geräten erlaubt. Der Anwender geht bedacht mit der Auswahl der Apps um und installiert insbesondere nur vom Anbieter verifizierte Apps.

⁴ Mobile Geräte dürfen in öffentlich zugänglichen Räumen nicht unbeaufsichtigt liegen gelassen werden.

⁵ Der Verlust eines mobilen Gerätes ist unverzüglich dem ISV zu melden.

Art. 17

Ausserbetriebnahme von IT-Geräten

Bei Ausserbetriebnahme von IT-Geräten der KGA mit einem Datenträger oder Übernahme zu Privat muss durch die Supportstelle eine Datenlöschung und Zurücksetzung der Profile beim Gerät vorgenommen werden.

Art. 18

Überwachung und Einschränkung der Nutzung

¹ Die Supportstelle trifft im Auftrag der KGA die geeigneten technischen Massnahmen zum Schutz der IT-Infrastruktur und zur Verhinderung missbräuchlicher Benutzung.

² Personenbezogene Daten werden bei Verdacht auf Missbrauch erst aufgrund einer ausdrücklichen durch die Strafverfolgungsbehörden angeordneten Zwangsmassnahme ausgewertet.

³ Bei Verstössen gegen dieses Reglement kann der ISV in Absprache mit der IT-verantwortlichen Person der KGA die Nutzung der IT-Infrastruktur einschränken.

⁴ Die KGA hat auch das Recht, Strafanzeige zu erstatten.

Art. 19

Support

Die KGA bezeichnet die Supportstelle.

Art. 20

Haftung

¹ Alle berechtigten Nutzer sind persönlich dafür verantwortlich, dass sie bei der Nutzung der IT-Infrastruktur nicht gegen dieses Reglement oder gegen die Rechtsordnung im Allgemeinen (Datenschutz, Strafrecht, etc.) verstossen und keine Rechte Dritter verletzt werden.

² Wer bei der Nutzung der IT-Infrastruktur schwerwiegende Unregelmässigkeiten (wie z.B. Missbräuche) feststellt, ist verpflichtet, diese so schnell wie möglich dem ISV zu melden.

³ Führen Verstösse gegen dieses Reglement zu Schäden an der IT-Infrastruktur bzw. zu erhöhtem Supportaufwand, wird eine Verrechnung der Aufwendungen an die verursachende Person geprüft. Die Haftung richtet sich hierbei analog nach Art. 321e OR.

⁴ Bei Verlust oder Beschädigung haftet die KGA. Dies aber nur, sofern der Nachweis erbracht wurde, dass der Schaden während der Arbeitszeit für die KGA erfolgt ist.

⁵ Die KGA übernimmt keine Haftung für Schäden, die Berechtigten aus der Benutzung der IT-Infrastruktur entstehen.

Art. 21

Ausnahmen

Der ISV entscheidet in Absprache mit der IT-verantwortlichen Person der KGA über Ausnahmen von vorliegendem Reglement. Entsprechende Gesuche sind dem ISV mit Begründung per E-Mail einzureichen.

Art. 22

Informationssicherheitsbeauftragter ISV

Der ISV ist im Organigramm der KG definiert. Bei einem Wechsel des ISV oder der in diesem Dokument definierten Richtlinien werden die Mitarbeitenden und Behördenmitglieder schriftlich informiert.

Art. 23

Inkrafttreten

Das vorliegende IT-Reglement tritt nach Ablauf der Referendumsfrist und der Genehmigung durch den Regierungsrat sofort in Kraft.

Katholischer Kirchgemeinderat Alpnach

der Kirchgemeindepräsident:

die Kirchgemeindeschreiberin:

Remo Kuster

Barbara Dall'Omo

Vom Regierungsrat, soweit an ihm, genehmigt am _____

Im Namen des Regierungsrates Obwalden

Mitgeltende Dokumente und Hilfsmittel:

- Antrag Hard-Software
- Bild und Videoaufnahme