Anlage 4



**Evangelische Kirchengemeinde xxxGemeindexxx**

Der Gemeindekirchenrat

Straße

PLZ Ort

Tel.: 00000/000000

 Fax: 00000/000000

 Mail: xxxxx@xxxxx.de

**Dienstanweisung
über die Nutzung elektronischer
Kommunikationssysteme am Arbeitsplatz
und den Umgang mit mobilen Datenträgern**

# Geltungsbereich und Zweckbestimmung

1. Diese Dienstanweisung regelt die Grundsätze für den Zugang und die Nutzung der Internetdienste in der Ev. Kirchengemeinde xxxGemeindexxx und gilt für alle hauptamtlich Tätigen.
2. Ziel dieser Vereinbarung ist die Herstellung der Transparenz der Nutzungsbedingungen und der Maßnahmen zur Protokollierung und Kontrolle, die Sicherung der Persönlichkeitsrechte der Beschäftigten und die Gewährleistung des Schutzes ihrer personenbezogenen Daten.

**Teil A – Nutzung elektronischer Kommunikationssysteme**

# Organisatorische Grundsätze

1. Die elektronischen Kommunikationssysteme stehen den Beschäftigten als Arbeitsmittel im Rahmen der Aufgabenerfüllung zur Verfügung.
2. Die Absicherung des Zuganges zum Internet wird durch eine Firewall des Netzbetreibers sichergestellt. Die Installation und Konfiguration von Web-Browsern, die IT-fachliche Betreuung der Beschäftigten sowie die Administration ihrer Internetberechtigungen erfolgt durch das IT-Funktionspersonal gem. IT-Sicherheitskonzept der Ev. Kirchengemeinde xxxGemeindexxx (Anlage 7).
3. Arbeitsplätze mit einem Internetzugang müssen wirksam durch Virenschutzprogramme vor Schadsoftware gesichert werden. Diese Programme dürfen durch Beschäftigte nicht eigenständig manipuliert oder deaktiviert werden. Gleiches gilt für den Einsatz von Filterprogrammen, die den Zugriff auf Angebote mit rechtswidrigen oder strafbaren Inhalten sperren, sowie für alle Sicherheitsprogramme und -einstellungen.

# Zulässigkeit der Nutzung

1. Die private Nutzung ist unter dem Vorbehalt des Widerrufs in geringfügigem Umfang zulässig, soweit die dienstliche Aufgabenerfüllung sowie die Verfügbarkeit des IT-Systems für dienstliche Zwecke nicht beeinträchtigt werden und die private Nutzung keine negativen Auswirkungen auf die Bewältigung der Arbeitsaufgaben hat.
2. Das Abrufen von Informationen oder Inhalten, die für die Kirchengemeinde Kosten verursachen, ist für den Privatgebrauch unzulässig. Im Rahmen der privaten Nutzung dürfen keine kommerziellen oder sonstigen geschäftliche Zwecke verfolgt werden.
3. Private E-Mails dürfen grundsätzlich nur über die Nutzung Webmail-Dienste versandt und empfangen werden. Über die dienstlichen E-Mail-Adressen eingehende private E-Mails sind wie private schriftliche Post zu behandeln. Eingehende private, aber fälschlich als Dienstpost behandelte E-Mails sind den betreffenden Beschäftigten unverzüglich nach Bekanntwerden ihres privaten Charakters zur alleinigen Kenntnis zu geben. Private E-Mails sind von Beschäftigten als solche zu kennzeichnen.
4. Eine Unterscheidung von dienstlicher und privater Nutzung auf technischem Weg erfolgt nicht. Die Protokollierung und Kontrolle gemäß Nr. 7 und 8 dieser Vereinbarung erstrecken sich auch auf den Bereich der privaten Nutzung des Internetzugangs. Die Beschäftigten erklären durch die private Nutzung des Internetzugangs seine Einwilligung in die Protokollierung und Kontrolle gemäß Nr. 7 und 8 dieser Vereinbarung für den Bereich der privaten Nutzung.
5. Dokumente, die personenbezogene oder andere sensible Daten beinhalten, dürfen nicht unverschlüsselt übertragen werden.
6. Das Ausführen von Programmen im Internet ist nur bei den vom IT-Verantwortlichen bekannt gegebenen Anbietern gestattet, soweit dies für den dienstlichen Gebrauch notwendig ist. Urheberrechtlich geschützte Dateien, für die keine Lizenz vorhanden ist, dürfen nicht abgerufen und gespeichert werden. Ermöglicht die Berechtigung der Beschäftigten das Abrufen und die Installation von Treibern, Setup-Programmen oder ähnlicher systemeingreifender Software, ist das vorher vom zuständigen IT-Verantwortlichen genehmigen zu lassen. Das Ausführen von aktiven Inhalten (z. B. Makros) in heruntergeladenen Dokumenten ist nur bei als vertrauenswürdig gekennzeichneten Anbietern gestattet. Die Einstellungen in den zugehörigen Anwendungen werden vom IT-Verantwortlichen vorgenommen.
7. Das Abrufen von kostenverursachenden Informationen oder Inhalten aus dem Internet bedarf der Genehmigung durch den GKR bzw. den Pfarrer.
8. Ferngesteuerte Zugriffe oder Steuerungen von Rechnersystemen über sogenannte Remote-Anwendungen bzw. Terminal-Emulationen (z. B. TeamViewer) sind grundsätzlich nicht zugelassen. Sollte dienstlicher Bedarf für Remote-Zugriffe bzw. Terminal-Emulationen bestehen, sind diese bei dem IT-Verantwortlichen unter Angabe der Gründe zu beantragen.
9. Mit Beendigung des Beschäftigungsverhältnisses steht die E-Mail-Adresse den jeweiligen Beschäftigten nicht mehr für diesen zur weiteren Nutzung zur Verfügung. Die Beschäftigten sind angehalten, ihre außerbetrieblichen Kommunikationspartner über diesen Umstand zu informieren. Dienstliche E-Mails werden an zur Aufrechterhaltung des Dienstbetriebes zuständige Beschäftigte weitergeleitet. Ist ein privater Charakter des Inhaltes dieser weitergeleiteten E-Mail ersichtlich, ist die E-Mail ohne weitere Kenntnisnahme des Inhaltes durch die jeweiligen Beschäftigten zu löschen. Eine Weiterleitung erfolgt nicht.
10. Aus Wirtschaftlichkeits- oder IT-Sicherheitsgründen kann die Internetnutzung beschränkt werden. Dies kann beispielsweise folgendes beinhalten:
* Sperrung bestimmter Dienste der Internetnutzung,
* Reduzierung auf bestimmte Internetanschlüsse,
* Beschränkung des Massendatentransfers oder des Speicherplatzes.

# Verhaltensgrundsätze

1. Die Beschäftigten haben jede Nutzung des Internets zu unterlassen, die geeignet ist, den Interessen der Kirchengemeinde oder deren Ansehen in der Öffentlichkeit zu schaden, die Sicherheit des landeskirchenweiten Intranets (LKI) zu beeinträchtigen oder die gegen geltende Rechtsvorschriften verstößt. Dies gilt vor allem für
* das Abrufen oder Verbreiten von Inhalten, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
* das Abrufen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen,
* die Nutzung des Internets zur Erledigung privater Rechtsgeschäfte, insbesondere die Nutzung von Zahlungsfunktionen (Onlinebanking, Internetversandhandel, eBay o.ä.) oder
* die Nutzung von Onlinespieleplattformen.

Abrufen und Aufrufen heißt auf im Netz vorhandene Informationen mit IT-Systemen der Kirchengemeinde zugreifen.

Verbreiten heißt Informationen einer Vielzahl von Personen oder einem unbestimmten Personenkreis über Internet-Dienste unter Verwendung von IT-Systemen der Kirchengemeinde anbieten.

1. Zur Überprüfung der Einhaltung der Regelungen dieser Vereinbarung können nicht-namensbezogene Stichproben (ohne Identifizierungsmerkmale) in den Protokolldateien durchgeführt werden. Ergänzend wird eine Übersicht über das jeweilige Gesamtvolumen des ein- und ausgehenden Datenverkehrs erstellt.
2. Die bei der Nutzung der Internetdienste anfallenden personenbezogenen Daten werden nicht zur Leistungs- und Verhaltenskontrolle verwendet. Sie unterliegen der Zweckbindung dieser Vereinbarung und den einschlägigen datenschutzrechtlichen Vorschriften.

# Information und Schulung der Beschäftigten

Die Beschäftigten werden durch die Kirchengemeinde über die besonderen Datensicherheitsprobleme bei der Nutzung der elektronischen Kommunikationssysteme unterrichtet und für den sicheren und wirtschaftlichen Umgang mit diesen Systemen fortgebildet.

# Verantwortlichkeit

Die Verantwortung für die Beachtung der vorgenannten Festlegungen und Hinweise obliegt den IT-Verantwortlichen sowie den jeweiligen Beschäftigten. Diese haben insbesondere auch sicherzustellen, dass eine Nutzung des Internets durch Unbefugte vom Arbeitsplatz aus nicht erfolgt.

**Hinweis:** Trotz des Einsatzes von Firewall oder Systemen und Software zum Schutz vor Schadsoftware ist das Ausspähen und Manipulieren von Daten durch Dritte nicht mit absoluter Sicherheit ausgeschlossen.

# Protokollierung und Kontrolle

1. Alle eingehenden E-Mails werden durch eine Firewall, einen Spam-Filter sowie Virenscanner geprüft.
2. Die Verkehrsdaten für den Internetzugang können mit Angaben von
* Datum/Uhrzeit,
* Adressen von Absender und Empfänger (z. B. IP-Adressen)
* Benutzeridentifikation (z. B. bei der Verwendung eines Proxy-Servers)
* der aufgerufenen Webseiten und
* übertragener Datenmenge

protokolliert werden.

1. Die Protokolle nach Absatz b. werden ausschließlich zu Zwecken der
* Analyse und Korrektur technischer Fehler
* Gewährleitung der Systemsicherheit
* Optimierung des Netzes
* statistischen Feststellung des Gesamtnutzungsvolumens
* Stichprobenkontrollen gemäß Absatz 4 und
* Auswertungen gemäß Nr. 8 dieser Vereinbarung (Missbrauchskontrolle)

verwendet.

1. Die Protokolle können durch die IT-Verantwortlichen der Kirchengemeinde regelmäßig stichprobenhaft hinsichtlich der aufgerufenen Websites, aber nicht personenbezogen, gesichtet und in aggregierter Form, also ohne Nennung von Namen und anderen Identifizierungsmerkmalen, ausgewertet werden.
2. Der Zugriff auf die Protokolldateien gemäß Absatz c. ist auf die IT-Verantwortlichen begrenzt. Diese haben eine entsprechende Verpflichtungserklärung zum Datenschutz unterschrieben. Darüber hinaus sind sie hinsichtlich der Einhaltung des Fernmeldegeheimnisses und des Datenschutzes auf die strafrechtlichen Konsequenzen bei Verstößen hingewiesen worden.
3. Die Protokolldaten werden nach 30 Tagen automatisch gelöscht.
4. Kontrolle und Auswertung von personenbezogenen Protokollen können sich auch auf die private Kommunikation erstrecken, da eine technische Trennung von privater und dienstlicher Kommunikation nicht erfolgt. Deshalb willigt jeder Beschäftigte mit der Unterzeichnung dieser Dienstvereinbarung in mögliche Eingriffe in das Fernmeldegeheimnis ein, die mit den unter a. genannten Maßnahmen verbunden sind. Außerdem werden die weiteren Rahmenbedingungen der Privatnutzung anerkannt.

# Maßnahmen bei Verstößen/Missbrauchsregelung

1. Bei Verdacht auf missbräuchliche oder unerlaubte Nutzung des Internetzugangs (hervorgerufen beispielsweise durch ein erhöhtes Gesamtdatenvolumen oder auch die Kenntnisnahme nicht zulässiger im Internet angebotener Inhalte) gemäß Nr. 3 und 4 dieser Vereinbarung durch einen Mitarbeiter erfolgt unter Beteiligung des GKR-Vorsitzenden eine Überprüfung des Datenverkehrs durch die IT-Verantwortlichen. Sind weitere Überprüfungen notwendig, werden diese von den in Satz 1 genannten Personen veranlasst. Auf der Basis dieser Untersuchung wird ein Bericht erstellt, der dem Betroffenen ausgehändigt wird. Dieser ist anschließend dazu zu hören.
2. Im Übrigen gelten die einschlägigen Regelungen des Disziplinar- bzw. Tarifrechts.
3. Ist aufgrund der stichprobenhaften nicht-personenbezogenen Kontrollen bzw. der Auswertung der Übersicht des Datenvolumens eine nicht mehr tolerierbare Häufung von offensichtlich privater Nutzung des Internetzugangs zu erkennen, so werden innerhalb einer zu setzenden Frist von zwei Wochen nach der Anhörung die Stichproben weiterhin nicht-personenbezogen durchgeführt.
4. Ergeben diese Stichproben bzw. die Auswertung der Übersicht des Datenvolumens keine Änderung im Nutzungsverhalten, so werden die Protokolle der folgenden zwei Wochen durch die in Absatz a. genannten Personen stichprobenhaft personenbezogen ausgewertet. Hierbei wird wie im Falle des Verdachts einer missbräuchlichen Nutzung vorgegangen. Zu den Verfahren nach Satz 1 und Satz 2 erfolgt eine entsprechende vorherige schriftliche Mitteilung an alle Beschäftigten, so dass deren Kenntnisnahme über die Maßnahmen gewährleistet werden kann.
5. Ein Verstoß gegen diese Dienstanweisung kann neben den dienst- und arbeitsrechtlichen Folgen auch strafrechtliche Konsequenzen haben.
6. Der GKR behält sich vor, bei Verstößen gegen diese Vereinbarung die private Nutzung des Internetzugangs im Einzelfall zu untersagen.

# Änderungen und Erweiterungen

Geplante Änderungen und Erweiterungen an den elektronischen Kommunikationssystemen werden den IT-Verantwortlichen mitgeteilt. Es wird dann geprüft, ob und inwieweit sie sich auf die Regelungen dieser Vereinbarung auswirken. Notwendige Änderungen oder Erweiterungen zu dieser Vereinbarung können im Einvernehmen in einer ergänzenden Regelung vorgenommen werden.

# Inkrafttreten

Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft. Sie kann mit einer Frist von zwei Wochen gekündigt werden. Im Falle einer Kündigung ist jede private Nutzung des Internetzuganges, auch der Empfang und das Versenden privater E-Mails über die dienstliche E-Mail-Adresse bis zum Abschluss einer neuen Vereinbarung untersagt.

**Teil B – Umgang mit mobilen Datenträgern**

# Begriffsbestimmung

Als mobile Datenträger werden externe und Wechselfestplatten, USB-Speichersticks, Speicherkarten, CD/DVD/Bluray, Disketten und Magnetbänder bezeichnet.

# Nutzung/Aufbewahrung von mobilen Datenträgern

1. Mobile Datenträger sind nur wenn unbedingt erforderlich einzusetzen.
2. Datenträger mit schutzwürdigem Inhalt sind in einem verschlossenen Schrank aufzubewahren.
3. Beim Aufbewahren von Datenträgern ist auf deren Haltbarkeit und Lagerbedingungen zu achten.
4. Das Einspielen von unbekannten Datenträgern darf erst nach Überprüfung auf Virenbefall erfolgen (Kontrolle bei Bedarf durch IT-Verantwortliche möglich).
5. Vertrauliche oder personengebundene Daten sind auf mobilen Datenträgern immer verschlüsselt zu speichern.
6. Bei Gebrauch in Fremd-PCs ist der Schreibschutz zu aktivieren (wenn möglich).
7. Es sind regelmäßig Virenprüfungen zu starten, besonders nach Gebrauch in Fremd-PCs.
8. Der Verlust eines mobilen Datenträgers ist an die IT-Verantwortlichen zu melden.

# Aussonderung/Vernichtung von mobilen Datenträgern

Beim Aussondern von mobilen Datenträgern sind diese physisch zu zerstören. Sie können dafür den IT-Verantwortlichen übergeben werden.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ort, Datum

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Unterschrift der/des Mitarbeitenden Unterschrift GKR-Vorsitzender

Original zur Personalakte

Kopie an die/den Mitarbeitenden