Mellingen
Stadt an der Reuss

Reglement über den Datenschutz und die Benutzung von Informatikmitteln

Der Gemeinderat Mellingen beschliesst

gestützt auf § 36 des Gesetzes über die Einwohnergemeinden (Gemeindegesetz, GG) sowie § 4 des Gesetzes über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) und der dazugehörenden Verordnung (VIDAG):

A. Grundsatz

§ 1 Zweck

1 Dieses Reglement steuert
a) den Zugang zu amtlichen Dokumenten
b) den Umgang mit Personendaten durch die Gemeinde
c) die Benutzung von Informatikmitteln der Gemeinde

2 Wo dieses Reglement nichts anderes bestimmt, gelten die übergeordneten Bestimmungen von Bund und Kanton.

§ 2 Geltungsbereich

Dieses Reglement gilt für alle dem Personalreglement der Gemeinde Mellingen unterstellten Mitarbeitenden und für die vom Volk gewählten Behörden und Kommissionen der Gemeinde Mellingen.

B. Zugang zu amtlichen Dokumenten

§ 3 Anwendbares Recht

Das anwendbare Recht und das Verfahren richten sich nach dem Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) sowie nach der dazugehörenden Verordnung (VIDAG).

§ 4 Entgegennahme des Gesuchs

1 Das Gesuch um Zugang zu amtlichen Dokumenten kann mündlich oder schriftlich bei der Gemeindekanzlei gestellt werden. Die Dokumente sind hinreichend genau zu bezeichnen.

2 Die Gemeindekanzlei leitet das Gesuch an diejenige Verwaltungsstelle oder Behörde weiter, welche das Dokument zuletzt bearbeitet hat.

§ 5 Gesuchsbehandlung und Entscheid

Über die Gewährung des Zugangs entscheidet der Abteilungsleiter oder die Behörde, welche das Dokument zuletzt bearbeitet hat gemäss Anhang 2 dieses Reglements.

C. Datenschutz

§ 6 Grundsatz

Die Datensicherheit, das Bekanntgeben von Daten, das Register der Datensammlungen und die Rechte der betroffenen Personen richten sich nach den übergeordneten Bestimmungen von Bund und Kanton.

§ 7 Begriff Personendaten

1 Der Begriff Personendaten umfasst alle Angaben über eine bestimmte oder bestimmbare natürliche oder juristische Person. Die Form der Bearbeitung und Darstellung der Personendaten ist dabei unwesentlich, geschehe sie nun manuell oder automatisch, auf Papier oder in Datenverarbeitungsanlagen.

2 Als Datensammlung wird in diesem Reglement jede systematische Sammlung von persönlichen oder sachlichen Daten bezeichnet, die nach den betroffenen Personen erschlossen ist.

§ 8 Zweckgebundenheit

1 Die Verwaltungsabteilungen dürfen Personendaten nur soweit sammeln, speichern oder anderweitig bearbeiten, wie dies für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist. Dies betrifft ebenfalls den Austausch der Daten unter den Verwaltungsabteilungen.

2 Besteht für eine Datensammlung keine gesetzliche Vorschrift, so regelt der Gemeinderat deren Zweck und Umfang.

3 Birgt die Bearbeitung von Personendaten besondere Risiken für die Persönlichkeitsrechte Betroffener, ist sie vorab der beauftragten Person für Öffentlichkeit und Datenschutz zu unterbreiten.

§ 9 Verantwortliche Verwaltungsabteilung

1 Für jede Datensammlung ist jene Verwaltungsabteilung verantwortlich, die diese für die Erfüllung ihrer Aufgaben benötigt. Sie ist für die Einhaltung dieses Reglementes verantwortlich.

2 Zugriff zu den Daten haben nur Mitarbeitende der administrativen Verwaltung. Sie sind zur Wahrung des Datenschutzes verpflichtet und haben nur im Rahmen ihrer Tätigkeit Zugang zu den Datensammlungen.

3 Der Gemeindeschreiber überwacht die Einhaltung des Datenschutzes in der Gemeinde.

§ 10 Grundsätze bei der Bearbeitung von Personendaten

1 Werden Personendaten beschafft, so ist dem Betroffenen stets der Zweck der Datensammlung bekannt zu geben.

2 Unrichtige und im Zweckbestimmungsverfahren unvollständige Personendaten sind zu berichtigen.

3 Personendaten, an deren Weiterbestand kein Bedarf mehr besteht, sind zu vernichten. Die Weisungen des Staatsarchivs sind einzuhalten.

§ 11 Weitergabe von Personendaten an öffentliche Organe

1 Personendaten werden im Einzelfall bekannt gegeben, wenn dafür eine Rechtsgrundlage besteht, dies zur Erfüllung einer rechtlichen Aufgabe des Organs erforderlich ist oder wenn die betroffene Person eingewilligt hat.

2 Besonders schützenswerte Personendaten dürfen bekannt gegeben werden, wenn dafür eine gesetzliche Grundlage besteht, dies im Einzelfall zur Erfüllung einer klar umschriebenen gesetzlichen Aufgabe erforderlich ist, die betroffene Person eingewilligt hat oder die Einwilligung der betroffenen Person nur mit unverhältnismässigem Aufwand erhältlich gemacht werden kann.

§ 12 Bekanntgabe von Daten an Private und Organisationen

1 Personendaten werden im Einzelfall bekannt gegeben, wenn dazu:
- eine gesetzliche Verpflichtung besteht
- die Bekanntgabe nötig ist, um eine gesetzliche Aufgabe erfüllen zu können
- die um Auskunft ersuchende Person glaubhaft macht, dass sie ohne Bekanntgabe an der Durchsetzung von Rechtsansprüchen gehindert wird
- die betroffene Person eingewilligt hat

2 Die Abteilung Einwohnerdienste kann privaten Dritten im Einzelfall auf Gesuch hin Personendaten bekannt geben, wenn diese berechtigte Interessen glaubhaft machen.

3 Personendaten können nach bestimmten Kriterien geordnet bekannt gegeben werden, wenn diese ausschliesslich für ideelle Zwecke verwendet werden und von privaten Dritten nicht weitergegeben werden.

4 Für die Bekanntgabe von nach bestimmten Kriterien geordneten Personendaten ist Anhang 1 dieses Reglementes zu beachten.

5 Jede Person kann schriftlich verlangen, dass die sie betreffenden Personendaten nicht an private Dritte weitergegeben werden. Die Datensperre ist den betroffenen Personen schriftlich zu bestätigen.

§ 13 Recht der Betroffenen

1 Jede Person kann bei der verantwortlichen Verwaltungsabteilung Auskunft verlangen, ob und welche Daten über sie in einer Datensammlung vorhanden sind.

2 Die Auskunft ist in allgemein verständlicher Form, in der Regel schriftlich, zu erteilen.

3 Die Auskunft darf eingeschränkt oder verweigert werden, soweit ein Gesetz oder überwiegende öffentliche oder private Interessen dies verlangen. Eine solche Einschränkung oder Verweigerung ist zu begründen.

4 Ergibt sich aus einer Anfrage, dass Personendaten unrichtig sind oder anderswie diesem Reglement widersprechen, so sind diese durch die verantwortliche Verwaltungsabteilung kostenlos zu berichtigen oder zu vernichten.

§ 14 Datensicherung

1 Die verantwortliche Verwaltungsabteilung trifft im Hinblick auf den Datenschutz organisatorische und technische Massnahmen, damit die Personendaten vor unbefugtem Zugriff und Verlust angemessen geschützt sind.

2 Für die elektronische Datensicherung ist der IT-Verantwortliche zuständig. Die Datensicherungen haben mindestens zweimal pro Woche zu erfolgen. Jeweils eine Sicherung ist extern zu lagern.

D. Benutzung von Informatikmitteln

§ 15 Persönliche Verantwortung

1 Alle Anwenderinnen und Anwender sind für die Verwendung der ihnen zur Verfügung gestellten Informatikmittel im Rahmen der geltenden Rechtsordnung und dieses Reglementes persönlich verantwortlich.

2 Feststellungen über technische Mängel und sicherheitsrelevante Vorkommnisse sind dem IT-Verantwortlichen sofort zu melden.

3 Der IT-Verantwortliche wird vom Gemeinderat bestimmt.

§ 16 Gebrauch von Informatikmitteln und E-Mail

1 Es dürfen grundsätzlich nur die vom IT-Verantwortlichen bereitgestellten Informatikmittel benutzt werden. Der Einsatz privater Informatikmittel ist nur mit Bewilligung des IT-Verantwortlichen zulässig.

2 Die Informatikmittel dürfen grundsätzlich nur zur Erfüllung dienstlicher Aufgaben benutzt werden.

3 Die Verwendung von Informatikmitteln zu privaten Zwecken soll zurückhaltend und grundsätzlich ausserhalb der ordentlichen Arbeitszeit unter Einhaltung der Vorschriften dieses Reglementes gehandhabt werden.

4 Benutzernamen und Passwörter sind persönlich und nicht übertragbar. Die Passwörter sind geheim zu halten und nach Anweisung des IT-Verantwortlichen regelmässig zu ändern.

5 Vertrauliche Informationen und Personendaten dürfen nicht ohne Einwilligung des Betroffenen per E-Mail übermittelt werden. Davon ausgenommen sind Übermittlungen an Amtsstellen, Behörden und Gemeindefunktionäre.

6 Das Versenden von privaten E-Mails ist nur unter Einhaltung der Vorschriften dieses Reglementes zulässig.

§ 17 Virenschutz

Der IT-Verantwortliche ist dafür besorgt, dass Server, Clients sowie alle weiteren erforderlichen Informatikmittel über ausreichend Schutz vor Viren etc. verfügen. Dies erfolgt in Rücksprache mit der für die IT beauftragten Firma.

§ 18 Berechtigungskonzept

Der IT-Verantwortliche erstellt die Benutzerprofile und weist den Mitarbeitenden die entsprechenden Benutzerrechte zu, welche sie zur Erfüllung ihrer Aufgaben benötigen.

§ 19 Abwesenheitsmeldungen

Bei Abwesenheiten von über 24 Stunden ist eine Abwesenheitsmeldung für eintreffende E-Mails einzurichten. Eintreffende E-Mails sind nicht weiterzuleiten, sondern die Adresse des Stellvertreters in der Abwesenheitsmeldung anzugeben.

§ 20 Unzulässiger Gebrauch der Informatikmittel

1 Missbräuchlich ist jede Verwendung der Informatikmittel, die
a) gegen dieses Reglement verstösst
b) gegen andere Bestimmungen der Rechtsordnung verstösst
c) Rechte Dritter verletzt

2 Missbräuchlich sind insbesondere folgende Handlungen:
a) Einrichten, Anschliessen oder Installation nicht bewilligter Informatikmittel und Verwendung oder Installation nicht bewilligter Programme
b) Versendung von E-Mails in Täuschungs-, Belästigungs- oder Beleidigungsabsicht und private Massensendungen
c) Zugriff auf Websites mit sexistischen, rassistischen oder pornographischem Inhalt sowie Erstellen von Links auf diese Websites
d) Widerrechtliches Kopieren von Daten und Software

§ 21 Nutzung WLAN im Rathaus

Im Rathaus Mellingen ist ein zugriffgeschütztes WLAN eingerichtet. Das WLAN kann von den Mitarbeitenden, den Gemeinderäten, Kommissionsmitgliedern sowie weiteren Nutzern des Verwaltungsbetriebes gratis verwendet werden (Public Area). Die Zugangsdaten werden vom IT-Verantwortlichen resp. dem Stv. verwaltet und herausgeben. Für den Zugriff auf das WLAN gelten dieselben Nutzungs- bzw. Sicherheitsbestimmungen des Reglementes über den Datenschutz und die Benutzung von Informatikmitteln.

§ 22 Kontroll- und Überwachungsmassnahmen

1 Kontroll- und Überwachungsmassnahmen dienen in erster Linie der Überprüfung und Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit und der Verfügbarkeit der Informatikmittel.

2 Zur Verhinderung von Missbrauch kann der Zugang zu bestimmten Internet-Adressen durch technische Massnahmen beschränkt oder verhindert werden.

§ 23 Sicherheit, Funktionsfähigkeit und Verfügbarkeit der Informatikmittel

1 Für die Anordnung von Kontroll- und Überwachungsmassnahmen zur Überprüfung und Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit und der Verfügbarkeit der Informatikmittel sowie die Durchführung von entsprechenden Auswertungen ist der IT-Verantwortliche zuständig. Diese Person hat dafür zu sorgen, dass solche Auswertungen nur von den dazu speziell autorisierten Systemverantwortlichen durchgeführt und streng vertraulich behandelt werden.

2 Die Protokolldaten sind in anonymisierter Form auszuwerten. Rückschlüsse auf bestimmte Anwenderinnen und Anwender dürfen nicht möglich sein.

3 Werden Störungen festgestellt, welche die technische Sicherheit, die Funktionsfähigkeit oder die Verfügbarkeit der Informatikmittel erheblich gefährden, dürfen die Protokolldaten ausnahmsweise personenbezogen ausgewertet werden, sofern dies zur Störungsbehebung unumgänglich ist. Die betroffenen Anwenderinnen und Anwender sind über die Tatsache und den Umfang der personenbezogenen Auswertung unverzüglich zu informieren.

4 Bei personenbezogenen Auswertungen hat der IT-Verantwortliche die vorgängige Einwilligung des Gemeinderates einzuholen und erstattet diesem sowie der beauftragten Person für die Öffentlichkeit und Datenschutz nachträglich Bericht über die durchgeführte Untersuchung und die allenfalls getroffenen Massnahmen. Kann eine Einwilligung vorgängig nicht eingeholt werden, darf die Auswertung durchgeführt werden, sofern die Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit oder der Verfügbarkeit der Informatikmittel keinen Aufschub erlaubt.

§ 24 Vollzug

1 Besteht erheblicher Verdacht auf Missbrauch der Informatikmittel, kann der Gemeinderat gegenüber einem begrenzten Personenkreis eine den Betroffenen schriftlich angekündigte, zeitlich befristete Kontrolle durchführen lassen.

2 Die Durchführung der Kontrollen hat unter Aufsicht des IT-Verantwortlichen zu geschehen. Die beauftragte Person für die Öffentlichkeit und Datenschutz ist vorgängig zu informieren und es ist ihr über die durchgeführte Untersuchung und allfällig getroffene Massnahmen nachträglich Bericht zu erstatten.

3 Die Auswertungsresultate werden ausschliesslich dem Gemeinderat und, sofern nötig, der vorgesetzten Person der oder des Betroffenen mitgeteilt.

E. Schlussbestimmungen und Inkrafttreten

§ 25 Kontrolle

Der Gemeinderat kontrolliert und überwacht die Einhaltung der Bestimmungen dieses Reglementes.

§ 26 Schlichtungsverfahren

Zieht die Behörde die teilweise oder vollständige Abweisung des Gesuchs gemäss Anhang 2 in Betracht, hat sie der gesuchsstellenden Person vorgängig Mitteilung zu machen. Diese ist berechtigt, innert 20 Tagen die beauftragte Person für Öffentlichkeit und Datenschutz um Schlichtung anzurufen.

§ 27 Rechtsschutz

Entspricht die Behörde dem Gesuch nicht vollumfänglich, erlässt sie eine begründete Verfügung mit Rechtsmittelbelehrung. Das Verfahren richtet sich nach dem Gesetz über die Verwaltungsrechtspflege (VRPG).

§ 28 Inkrafttreten

Dieses Reglement tritt per 01. Februar 2016 in Kraft und ersetzt das Reglement über den Datenschutz vom 28. März 1983 (ergänzt 19.12.1988).

Genehmigt an der Sitzung vom 18. Januar 2016.

Gemeinderat Mellingen
Der Gemeindeammann:

Bruno Gretener
Der Gemeindeschreiber:

Patrick Sandmeier

Anhang 1: Bekanntgabe von Personendaten
Anhang 2: Gesuch um Zugang zu amtlichen Dokumenten bzw. Informationen
Anhang 3: Richtlinien für Social Media

Anhang 1
Bekanntgabe von Personendaten

Anspruchsberechtigte Personen

Folgende nach bestimmten Kriterien geordnete Personendaten werden für ideelle Zwecke unentgeltlich zur Verfügung gestellt:

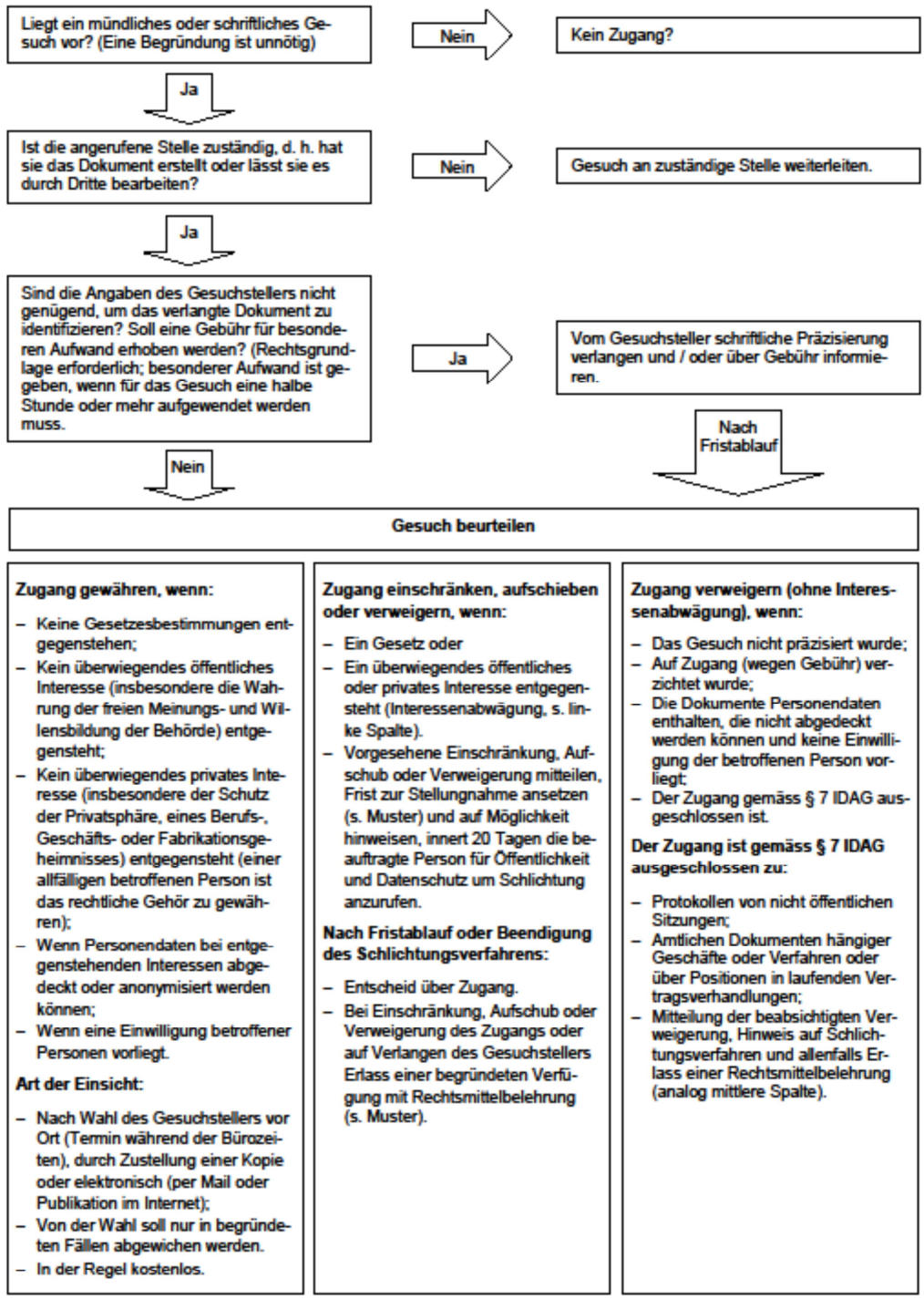
- Ortsansässige Vereine und Organisationen (Sitz in Mellingen gemäss Statuten) zur Förderung des Gemeinschaftslebens, der Gesundheitsvorsorge, des Sports oder der Kultur
- Liste der Geburten für die Mütter- und Väterberatungsstelle
- Organisationen mit öffentlichem Zweck zur Mitgliederwerbung und für Spendenaufruf; das ZEWO-Gütesiegel oder die entsprechende Anerkennung durch das Steueramt des Kantons Aargau gilt als Nachweis für die Gemeinnützigkeit
- Adresslisten für Kirchgemeinden zum Eigengebrauch
- Stimmregister-Listen für Kirchgemeinden
- Adresslisten für Feuerwehr, Polizei und Zivilschutz

Anhang 2
Gesuch um Zugang zu amtlichen Dokumenten bzw. Information

Gesuchsprüfung

Über die Gewährung des Zugangs entscheidet der Abteilungsleiter oder die Behörde, welche das Dokument zuletzt bearbeitet hat.

Zugangsrecht – Schema 2:
Prüfung Gesuch um Zugang zu amtlichen Dokumenten



Anhang 3
Richtlinien für Social Media

Social Media helfen, mit Menschen in Kontakt zu bleiben, vereinfachen die Kommunikation und helfen transparente, authentische Unternehmensbilder zu zeichnen. Doch bei allen Vorteilen bergen Social Media auch Risiken. Deshalb ist ein verantwortungsbewusster Umgang im geschäftlichen wie auch privaten Alltag wichtig.

Denken Sie immer daran, dass alles in den Social Media, was Sie eingeben, auch recherchiert werden kann, beruflich wie privat (Facebook, Twitter, YouTube, Google, Xing, Blogs usw.). Anbei einige Regeln:

1. **Wer veröffentlicht übernimmt Verantwortung.** Sie sind für Ihre veröffentlichten Meinungsäusserungen selbst verantwortlich. Jede Veröffentlichung kann von Kunden, Partnern oder Journalisten aber auch von Vorgesetzten, Kollegen oder ehemaligen Mitarbeitenden gelesen werden. Eine Veröffentlichung bleibt immer im Internet bestehen. Diese zu löschen ist fast unmöglich und kann weitreichende Konsequenzen haben.

2. **Schonen Sie Ihre Geschäftsbeziehungen.** Selbst wenn Kunden und Partner Ihnen Stress und Ärger bereiten, sollten Sie niemals Ihren persönlichen Frust in der Öffentlichkeit ablassen. Negatives oder Respektloses über Kunden, Geschäftspartner, Mitbewerber oder Produkte zu verbreiten ist tabu.

3. **Verraten Sie keine Geschäftsgeheimnisse.** Schreiben Sie nichts, was nicht für Aussenstehende bestimmt ist. Halten Sie sich an die entsprechenden Weisungen Ihres Arbeitgebers. Wenden Sie sich im Zweifelsfall an Ihre Vorgesetzten oder die entsprechende Stelle.

4. **Seien Sie authentisch.** Geben Sie sich immer mit vollständigem Vor- und Nachnamen, Funktion und Unternehmen zu erkennen, sofern die veröffentlichten Inhalte Ihre Arbeit betreffen. Machen Sie zu Ihrem eigenen Schutz und dem Schutz der Gemeinde deutlich, wenn Sie sich als Privatperson äussern.

5. **Umgangston.** Behandeln Sie andere Nutzer so, wie Sie selbst behandelt werden möchten. Argumentieren Sie in der Sache nie mit persönlichen Angriffen oder Argumenten, die sich auf Personen beziehen. Beleidigungen, sexuelle Anspielungen oder rassistische Äusserungen sind gesetzlich untersagt.

6. **Offen mit Fehlern umgehen.** Fehler oder Fehleinträge müssen proaktiv und konstruktiv kommentiert werden. Sprechen Sie im Zusammenhang mit der Gemeinde im Zweifelsfall mit Ihrem Vorgesetzten oder der entsprechenden Stelle. Einen Fehler einzugestehen ist besser als der Versuch der Rechtfertigung, Vertuschung oder deren Löschung.

7. **Social Media Einsatz während der Arbeitszeit.** Die private Nutzung von Social Media während der Arbeitszeit ist untersagt. Die geschäftliche Nutzung ist mit Ihren Vorgesetzten zu klären.

8. **Ziele.** Prüfen Sie jeweils, ob Ihre beruflichen Social Media Aktivitäten mit den Zielen oder Leitbildern übereinstimmen und einen Mehrwert für die Gemeinde schaffen.