

EINWOHNERGEMEINDE MURGENTHAL



REGLEMENT ÜBER DIE BENÜTZUNG VON INFORMATIKMITTELN DER GEMEINDE

Stand: 27.9.2021

Reglement des Gemeinderates über die Benutzung von Informatikmitteln der Gemeinde

vom 2. März 2015

Der Gemeinderat,

gestützt auf § 4 der Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen vom 26. September 2007 (VIDAG)¹

beschliesst:

§ 1

Geltungsbe-
reich

¹ Dieses Reglement gilt für die Behörden der Gemeinde Murgenthal, insbesondere für die Mitglieder des Gemeinderates, die Mitglieder der Kommissionen sowie die Mitarbeitenden der Gemeindeverwaltung, soweit ihnen die Gemeinde Informatikmittel zur Verfügung stellt.

² Dieses Reglement gilt nicht für die Schule.

§ 2

Zweck

¹ Das Reglement ordnet die Benutzung von Informatikmitteln der Gemeinde.

² Es hat zum Zweck, die Datenbestände zu schützen, den sicheren und wirtschaftlichen Einsatz der Informatikmittel zu gewährleisten sowie die Persönlichkeitsrechte der Anwenderinnen und Anwender zu wahren.

¹ SAR 150.711

§ 3

Informatikver-
antwortliche/r

¹ Der Gemeinderat ernennt eine/n Informatikverantwortliche/n und eine/n Stellvertreter/in.

² Der/die Informatikverantwortliche ist für den reibungslosen Betrieb der Informatikmittel und für den 1st-Level-Support verantwortlich. Sie/er wird bei dieser Aufgabe im Rahmen von Service- und Wartungsverträgen, für deren Abschluss der Gemeinderat zuständig ist, von externen Fachleuten unterstützt.

§ 4

Daten-
sicherung

¹ Für die Datensicherung ist der/die Informatikverantwortliche zuständig. Er/sie kann Instruktionen und Weisungen zuhanden der Anwenderinnen und Anwender erlassen.

Informatikver-
antwortliche/r

² Die auf dem Server gespeicherten Daten sind so zu sichern, dass sie nach einer Zerstörung der Anlage oder einer unbeabsichtigten Löschung mit hoher Wahrscheinlichkeit und mit verhältnismässigem Aufwand wieder hergestellt werden können.

³ Es sind mehrere Generationen von Datensicherungen anzulegen. Die Sicherungs-Datenträger sind vor Diebstahl und Elementarschaden geschützt aufzubewahren.

⁴ Mindestens einmal wöchentlich ist ein Sicherungs-Datenträger an einen gesicherten Aufbewahrungsort ausserhalb des Gebäudes, in welchem sich der Server befindet, zu bringen (z. B. in ein Bank-Tresorfach). Dritte dürfen keinen Zugriff zu diesen Datenträgern erhalten.

§ 4a

Datensiche-
rung in die
Cloud

Die Datensicherung auf externe Server ist zulässig, wenn alle Server ihren Standort in der Schweiz haben und das Vertragsverhältnis schweizerischem Recht untersteht. Die Daten sind verschlüsselt zu übermitteln.

§ 5

Anwender
/innen

¹ Die Daten sind von den Anwenderinnen und Anwendern auf dem Server zu speichern. Die Speicherung von Daten auf der lokalen Festplatte ist zu unterlassen.

² Für die Sicherung der Einstellungen der Arbeitsplatz-Computer und allfälliger auf der lokalen Festplatte abgelegter Dateien sind die Anwenderinnen und Anwender verantwortlich.

§ 6

Persönliche
Verantwortung

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

² Feststellungen über technische Mängel und sicherheitsrelevante Vorkommnisse sind der/dem Informatikverantwortlichen sofort zu melden.

§ 7

Gebrauch von
Informatik-
mitteln

¹ Es dürfen grundsätzlich nur die vom/von der Informatikverantwortlichen bereitgestellten Informatikmittel benutzt werden. Der Einsatz privater Informatikmittel ist nur mit Bewilligung des/der Informatikverantwortlichen zulässig.

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

³ Die Verwendung von Informatikmitteln der Gemeinde zu privaten Zwecken ist nur ausserhalb der Arbeitszeit und unter Einhaltung der Vorschriften dieses Reglements zulässig. Es dürfen keine Programme installiert werden, die ausschliesslich privaten Zwecken dienen.

⁴ Benutzernamen und Passwörter sind persönlich und nicht übertragbar. Die Passwörter sind geheim zu halten und nach Anweisung des/der Informatikverantwortlichen regelmässig zu ändern.

§ 7a

WLAN-Netz für
Gäste

¹ Im Gemeindehaus besteht ein WLAN-Netz für Gäste. Dieses bietet Zugang zum Internet. Auf die nicht-öffentlichen Server der Gemeindeverwaltung kann über das WLAN-Netz nicht zugegriffen werden.

² Das WLAN-Netz kann von den Mitarbeitenden der Gemeinde mitbenutzt werden. Es dürfen private Informatikmittel eingesetzt werden, in den Pausen und ausserhalb der Arbeitszeiten auch zu privaten Zwecken.

³ Für den Zugriff zum WLAN-Netz wird ein zeitlich befristetes Passwort vergeben. Pro Passwort können höchstens zwei Geräte an das WLAN-Netz angeschlossen werden.

⁴ Die über das WLAN-Netz getätigten Internet-Zugriffe werden protokolliert. § 10 dieses Reglements gilt sinngemäss.

§ 7b

Home-Office

¹ Für die Arbeit von zu Hause aus können private Informatikmittel eingesetzt werden, sofern sie über ein aktuelles Betriebssystem und über einen aktuellen Virenschutz verfügen.

² Für die Einwahl auf den Server der Gemeinde ist eine Zwei-Faktor-Authentisierung zu verwenden.

³ Für das blosses Abrufen von E-Mails und Terminen genügt die Identifizierung mittels Passwort.

§ 8

Gebrauch von
E-Mail

¹ Vertrauliche Informationen und Personendaten dürfen grundsätzlich nicht ohne Einwilligung des/der Betroffenen per E-Mail übermittelt werden. Zulässig ist die Übermittlung innerhalb der Domain @murgenthal.ch sowie über vom Kanton zur Verfügung gestellte verschlüsselte E-Mail-Verbindungen. Müssen Personendaten infolge Dringlichkeit ausnahmsweise doch über eine ungeschützte E-Mail-Verbindung übermittelt werden, ist die Datei mit einem Passwort zu versehen.

² Private E-Mails, die über das Postfach der Gemeinde verschickt werden, sind im Betreff mit "Privat" zu kennzeichnen.

³ Der Gebrauch privater E-Mail-Adressen ist nur mit Bewilligung des/der Informatikverantwortlichen zulässig.

§ 9

Abwesenheitsmeldungen

Bei Abwesenheiten von mehr als einem Arbeitstag ist eine Abwesenheitsmeldung für eintreffende E-Mails einzurichten. Eintreffende E-Mails sind nicht weiterzuleiten, sondern es ist in der Abwesenheitsmeldung die Adresse der Stellvertreterin oder des Stellvertreters anzugeben.

§ 10

Unzulässiger Gebrauch der Informatikmittel

¹ Unzulässig ist jede Verwendung der Informatikmittel, die

- a) gegen dieses Reglement verstösst,
- b) gegen andere Bestimmungen der Rechtsordnung verstösst,
- c) Rechte Dritter verletzt.

² Unzulässig 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 sexistischem, rassistischem oder pornographischem Inhalt sowie Erstellen von Links auf diese Websites,
- d) widerrechtliches Kopieren von Daten oder Software.

§ 11

Kontroll- und Überwachungs-massnahmen

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

² Zur Gewährleistung der Sicherheit und der Kapazitäten des Netzwerks sowie zur Verhinderung von Missbrauch kann der Zugang zu bestimmten Internet-Adressen durch technische Massnahmen beschränkt oder verhindert werden.

³ Der Inhalt privater E-Mails darf ohne Zustimmung der betroffenen Anwenderinnen und Anwender nicht gelesen werden.

§ 12

Sicherheit,
Funktionsfähigkeit
und
Verfügbarkeit
der Informatikmittel

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

² Werden Störungen festgestellt, welche die technische Sicherheit, die Funktionsfähigkeit oder die Verfügbarkeit der Informatikmittel erheblich gefährden, dürfen Protokolldaten 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.

³ Bei personenbezogenen Auswertungen hat die oder der Informatikverantwortliche die vorgängige Einwilligung des Gemeinderates einzuholen. Er/sie erstattet dem Gemeinderat sowie der beauftragten Person für 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.

§ 13

Vollzug

¹ Besteht erheblicher Verdacht auf Missbrauch von Informatikmitteln, 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/der Informatikverantwortlichen zu geschehen. Die beauftragte Person für 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 Auswertungsergebnisse werden ausschliesslich dem Gemeinderat und, sofern nötig, der vorgesetzten Person des/der Betroffenen mitgeteilt.

§ 14

Inkrafttreten

Dieses Reglement tritt am 1. April 2015 in Kraft. Es wird den Anwenderinnen und Anwendern der gemeindeeigenen Informatikmittel ausgehändigt.

4853 Murgenthal, 2. März 2015

GEMEINDERAT MURGENTHAL

Gemeindeammann Gemeindeschreiber

Max Schärer Rolf Wernli

Änderungstabelle

Element	Änderung	Beschluss	Inkrafttreten
§ 1 Abs. 2	eingefügt	27.9.2021	27.9.2021
§ 4a	eingefügt	27.9.2021	27.9.2021
§ 7a	eingefügt	10.12.2018	10.12.2018
§ 7b	eingefügt	27.9.2021	27.9.2021