Nutzungsvereinbarung für ein gemeindeeigenes Tablet im Zusammenhang mit der Nutzung von Session (Sitzungsmanagement)

1. Einführung

Am 14.11.2019 hat der Gemeinderat beschlossen, dass die Mitglieder des Gemeinderats Einladungen und Sitzungsunterlagen alternativ auch elektronisch erhalten können. Auf Antrag wird hierfür ein Tablet zur Verfügung gestellt.

Mit dieser Maßnahme sollen Kosten eingespart werden und eine frühzeitige und digitale Verfügbarkeit der Sitzungsunterlagen ermöglicht werden. Sitzungsvorlagen und Beschlüsse zurückliegender Sitzungen werden ebenfalls elektronisch zugänglich gemacht. Für Sitzungen im Sitzungssaal des Rathauses wird hierzu ein Internetzugang zur Verfügung gestellt.

Diese Nutzungsbedingung umfasst technische und organisatorische Regelungen, um die Sicherheit und den ordnungsgemäßen Umgang mit den Tablets in der Gremienarbeit des Gemeinderats zu gewährleisten.

2. Geltungsbereich

Diese Nutzungsbedingungen gelten für Mitglieder des Gemeinderats und Ortsvorsteher (Nutzer), welche sich für die Nutzung eines gemeindeeigenen Tablets entschieden haben.

3. Voraussetzungen

Für die Nutzung des Tablets müssen eine persönliche E-Mailadresse, sowie ein sicherer und leistungsfähiger WLAN-Zugang (kein öffentlicher Hotspot; empfohlene Bandbreite min. 6Mbit/s) für das Internet zur Verfügung stehen.

Die Sitzungseinladungen, Unterlagen und Beschlüsse werden elektronisch zur Verfügung gestellt. Die Bereitstellung schriftlicher Unterlagen entfällt.

Die Stadt Hüfingen bleibt alleinige Eigentümerin der in der Nutzungsvereinbarung aufgeführten Hard- und Software.

4. Begriffsbestimmungen

Technische Begriffe werden in der Begriffserläuterung (Anhang) näher erläutert.

5. Nutzung des Tablets

5.1 Dienstliche Nutzung

Das Tablet ist für die Arbeit im Gemeinderat und dessen Ausschüsse vorgesehen.

5.2 Private Nutzung

Die Nutzer können das Tablet auch privat nutzen.

Mit dem Gerät soll sorgsam und gewissenhaft umgegangen werden. Es ist nicht erlaubt, sicherheitsgefährdende Applikationen (Apps) auf dem Gerät zu installieren und zu benutzen, bzw. einen sogenannten Jailbreak vorzunehmen. Datenzugriffe im Internet dürfen nicht gegen Gesetze verstoßen; insbesondere dürfen nur Dateien und Programme heruntergeladen und gespeichert werden, welche nicht gegen das Urheberrecht verstoßen. Die Verantwortung für den rechtmäßigen Gebrauch trägt der Nutzer.

Die Weitergabe und Verwendung des Geräts durch Dritte ist untersagt.

6. Beschaffung, Kosten und Haftung

6.1 Beschaffung

6.1.1 Hardware

Die EDV-Abteilung der Stadt Hüfingen definiert den einzuhaltenden Gerätezustand. Die Geräte werden zentral beschafft und zur Verfügung gestellt.

6.1.2 Dienstliche Software

Dienstliche Software wird durch die Stadt Hüfingen zur Verfügung gestellt. Zunächst ist der elektronische Sitzungsdienst mit dem Programm „Session“ vorgesehen. Dieses wird von der Stadt Hüfingen installiert. Falls weiter dienstliche Apps notwendig sind, erfolgt die Installation ebenfalls durch die Stadt Hüfingen.

6.1.3 Private Software

Die Installation privater Software ist grundsätzlich erlaubt, sofern diese die Sicherheit des Gerätes und der darauf gespeicherten Daten nicht gefährdet. Der Nutzer hat selbst für eine zweckmäßige Ablage zu sorgen und ist selbst für die Datensicherung verantwortlich. Er trägt Sorge dafür, dass sensible Daten Dritten nicht zugänglich gemacht werden. Die Sicherheitssysteme müssen installiert und aktiviert bleiben.
Die Stadt Hüfingen behält sich das Recht vor, den Gebrauch privater Software zu untersagen.

6.2 Haftung

Für Schäden, welche während der vorgesehenen Nutzung des mobilen Gerätes entstehen, übernimmt die Stadt Hüfingen die anfallenden Reparaturkosten oder gegebenenfalls den Ersatz des Gerätes.

Handelt ein Nutzer grob fahrlässig oder vorsätzlich, muss er anfallende Kosten teilweise oder ganz tragen. Dies gilt insbesondere für Schäden, die auf einen unsachgemäßen Gebrauch des Gerätes zurückzuführen sind.

Entstehen durch die private Nutzung rechtliche Folgen, sind diese eigenverantwortlich vom Nutzer zu tragen.

7. Laufender Betrieb

7.1 Erklärung

Die Nutzer verpflichten sich, die nachfolgenden Handlungsrichtlinien einzuhalten und zu beachten.

7.2 Organisatorische Maßnahmen

Zur Verwendung der Tablets müssen -insbesondere aus datenschutzrechtlichen Gründen- Sicherheitsmaßnahmen eingehalten werden.

7.2.1 Allgemeiner, sicherer Umgang

- Um eine Grundsicherheit zu gewährleisten, wird ein Geräte-Passwort festgelegt.
- Dieses muss mindestens 8 Zeichen beinhalten.
- Das Passwort muss alle 90 Tage erneuert werden.
- Nach fünfmaliger Falscheingabe des Gerätepassworts, wird das Gerät automatisch auf seine Werkseinstellungen zurückgesetzt. Hierbei werden alle Daten gelöscht.
- Eine Weitergabe des Gerätepassworts ist nicht erlaubt.
- Das Gerätepasswort darf nicht zusammen mit dem Gerät aufbewahrt werden.
- Der Zugriff und die Verwaltung der elektronischen Sitzungsunterlagen erfolgt mit dem Programm „Sessions“. Die bei Anmeldung notwendigen persönlichen Informationen dürfen keinesfalls weitergegeben werden.
- Das Gerät darf nicht unbeaufsichtigt liegen bleiben und muss sicher aufbewahrt werden, um es vor unberechtigten Zugriffen dritter zu schützen.
- Schnittstellen, wie WLAN oder Bluetooth müssen nach Gebrauch sofort deaktiviert werden, da sie ein Sicherheitsrisiko darstellen können.
- Der Verlust des Gerätes ist umgehend bei der Stadt Hüfingen anzuzeigen. Ortungsdienste sollen aus Datenschutzgründen grundsätzlich nicht aktiviert werden. Auf ausdrücklichen Wunsch des Nutzers können diese in Einzelfällen eingeschaltet werden.

7.2.2 Internetverbindung

Eine Datenverschlüsselung ist zwingend und muss mindestens dem WPA-Standard entsprechen. Die Nutzung öffentlicher Hotspots und ungesicherter/ unverschlüsselter WLAN-Netze ist untersagt.

7.3 Datensicherung und Datenschutz

Dienstliche Daten werden generell primär auf zentralen Systemen gehalten und verwaltet. Auf den mobilen Geräten liegen sie nur temporär oder als Duplikat. Daher werden Daten auf den mobilen Geräten seitens der Stadt Hüfingen nicht gesichert.

Der Anschluss an einen privaten Computer darf nur erfolgen, wenn dieser mit einem aktuellen Virenschutz ausgestattet ist.

Der Computer muss vor fremden Zugriffen ausreichend geschützt sein.

Die Vorschriften des Landes- und Bundesdatenschutzgesetzes (LDSG, BDSG, DSGVO), sowie der Gemeindeordnung Baden-Württemberg sind zu beachten.

7.3.1 Konfiguration der Geräte

Die Erstkonfiguration des Gerätes wird durch die Stadt Hüfingen durchgeführt.

7.3.2 Updates

Die Stadt Hüfingen informiert die Nutzer über die für ihr Gerät erforderlichen Updates (Firmware, Betriebssystem). Der Nutzer ist verpflichtet, dies zeitnah umzusetzen.

Die Stadt Hüfingen informiert die Nutzer über Updates von dienstlichen Anwendungen. Diese werden soweit möglich automatisiert verteilt. Alle anderen Anwendungen hat der Nutzer zeitnah auf den aktuellen Stand zu bringen.

7.3.3 Verschlüsselung von Datenträgern

Die Verschlüsselung von auf dem Gerät gespeicherten sensiblen bzw. personenbezogenen Daten ist mit gegebenen Mittel zu gewährleisten. Dies wird i.d.R. vor der Auslieferung von der Stadt Hüfingen konfiguriert.

7.3.4 Viren- und Malwareschutz (für Android/ Windows Geräte)

Jedes mobile Gerät wird mit erforderlichen und möglichen Viren- und Malwareschutzfunktionen ausgeliefert. Diese dürfen nicht vom Gerät entfernt werden.

Soweit technisch möglich erfolgt die Aktualisierung dieser Funktionen automatisiert. Sofern dies nicht möglich ist, hat der Nutzer die Funktionen zeitnah auf den aktuellsten Stand zu bringen.

7.4. Unterstützung

7.4.1 Probleme mit dem Gerät und dessen Handhabe

Die Nutzer erhalten bei der Ausgabe des Geräts eine Einweisung.

Für Fragen im Rahmen der technischen, dienstlichen Nutzung des Tablets steht Ihnen die EDV-Abteilung der Stadt Hüfingen zur Verfügung (Mail Support).

7.4.2 Schadensfall

Der Nutzer trägt dafür Sorge, dass Schäden, die am Gerät auftreten, unverzüglich der Stadt Hüfingen gemeldet werden. Zwecks Schadensanalyse und Reparatur ist das Gerät der Stadt Hüfingen zu überlassen. Sofern verfügbar, wird ein Ersatzgerät zur Verfügung gestellt.

Ist das Gerät defekt und kann nicht mehr repariert werden, ist das entsprechende Gerät bei der Stadt Hüfingen abzugeben und ein neues Gerät zu beantragen.

7.5 Verhalten bei Verlust

Ein Verlust des Gerätes ist unverzüglich der EDV-Abteilung der Stadt Hüfingen zu melden. Weitere Maßnahmen, wie die Sperrung und Fernlöschung des Gerätes, werden durch den zuständigen Sachbearbeiter durchgeführt.

7.6 Rückgabe, Außerbetriebnahme und Entsorgung

7.6.1 Ende der Nutzung

Endet die Mitgliedschaft im Gemeinderat oder die ehrenamtliche Tätigkeit als Ortsvorsteher, ist das Gerät bei der Stadt Hüfingen abzugeben. Das Gerät wird dann auf seine Werkseinstellungen zurückgesetzt, so dass keine persönlichen Daten mehr vorhanden sind.

8. Inkrafttreten

Diese Nutzungsvereinbarung tritt mit Unterzeichnung in Kraft.

Hüfingen, den

Michael Kollmeier

Bürgermeister

Gemeinderat/Ortsvorsteher

Anhang: Begriffserläuterungen

Apps*	Aus dem englischen Begriff application hat sich in der Alltagssprache auch die Bezeichnung Applikation, kurz App, eingebürgert. Im deutschen Sprachraum wird die Abkürzung App seit dem Erscheinen des iOS App Store (2008) fast ausschließlich mit mobiler App gleichgesetzt, also Anwendungssoftware für Mobilgeräte wie Smartphones und Tablet-Computer. Allerdings wird inzwischen auch teilweise Desktop-Anwendungssoftware App genannt, z. B. beim Betriebssystem Microsoft Windows 8 (Windows-Apps), das sowohl auf Desktop-PCs als auch Tablet-PCs eingesetzt wird.
App-Store*	App Store (von der englischen Kurzform für Application = Computerprogramm und Store = Geschäft; auch Appstore, Application Store, App Market) ist die Bezeichnung für eine digitale Vetriebsplattform von Anwendungssoftware. Der Service ermöglicht es Benutzern Software aus einem Anwendungskatalog von Erst- und Drittanbieterentwicklern zu suchen und herunterzuladen.
BYOD*	BYOD („Bring Your Own Device“) ist die Bezeichnung dafür, private mobile Endgeräte wie Laptops, Tablets oder Smartphones in die Netzwerke von Unternehmen oder Schulen, Universitäten und anderen (Bildungs-) Institutionen zu integrieren.
Firmware*	Als Firmware bezeichnet man sowohl die Betriebssoftware diverser Geräte oder Komponenten (z. B. Mobiltelefon, Spielkonsole, Fernbedienung, Festplatte, Drucker) als auch die grundlegende Software eines Computers (z. B. das in einem Flash-Speicher verankerte BIOS bei Personalcomputern), die notwendig ist, um den Betriebssystemkern des eigentlichen Betriebssystems laden und betreiben zu können.
Hotspot*	Hotspots sind öffentliche drahtlose Internetzugriffspunkte, die (oft gegen Bezahlung) für jedermann zugänglich sind. Die meisten sind im öffentlichen Raum installiert: in Restau-rants, Cafés, Bibliotheken, Hotels, Krankenhäusern oder öffentlichen Plätzen (Flughäfen, Bahnhöfen usw.). Mit einem Notebook, PDA oder Mobiltelefon kann man mittels der WLAN-Technologie eine Verbindung zum Internet aufbauen.
Jailbreak*	Jailbreak (englisch; dt.: „Gefängnisausbruch“) bezeichnet das nicht-autorisierte Entfernen von Nutzungsbeschränkungen bei Geräten der Informationstechnik, deren Hersteller bestimmte Funktionen serienmäßig gesperrt hat. Der Begriff entstand ursprünglich mit Bezug auf die Virtualisierungsumgebung von FreeBSD. Populär wurde er jedoch erst durch den Jailbreak der Apple-Mobilgeräte, die das iOS-Betriebssystem verwenden (iPhone, iPod Touch, iPad und AppleTV), da Apple ein striktes „Closed World“-Geschäftsmodell verfolgt – was unter anderem bedeutet, dass auf den Geräten ausschließlich Software aus dem firmeneigenen App Store installiert werden kann.
Malware*	Malware ist damit ein Oberbegriff, der u. a. den Computervirus umfasst. Der Begriff des Virus ist älter und häufig nicht klar abgegrenzt. So ist die Rede von Virenschutz, womit viel allgemeiner der Schutz vor Schadsoftware jeglicher Art gemeint ist. Ein typischer Virus verbreitet sich, während die heute gängigen Schadprogramme die Struktur von Trojanischen Pferden zeigen, deren primärer Zweck nicht die Verbreitung, sondern die Fernsteuerbarkeit ist.

Mobile Endgeräte*	Mobile Endgeräte bzw. Mobilgeräte sind Endgeräte, die aufgrund ihrer Größe und ihres Gewichts ohne größere körperliche Anstrengung tragbar und somit mobil einsetzbar sind. Endgeräte sind hier ausschließlich in ihrer informationstechnischen und kommunikations-technischen Definition zu verstehen.
PIN*	Eine Persönliche Identifikationsnummer (PIN) oder Geheimzahl ist eine nur einer oder wenigen Personen bekannte Zahl, mit der diese sich gegenüber einer Maschine authentisieren können.
Remote	Fernzugriff auf Geräte
SIM*	Die SIM-Karte (vom englischen subscriber identity module für „Teilnehmer-Identitätsmodul“) ist eine Chipkarte, die in ein Mobiltelefon eingesteckt wird und zur Identifikation des Nutzers im Netz dient. Mit ihr stellen Mobilfunkanbieter Teilnehmern mobile Telefonanschlüsse und Datenanschlüsse zur Verfügung. Das SIM ist ein kleiner Prozessor mit Speicher (üblicherweise im ID-000-Format, das aus einer ID-1-Format-Karte herausgebrochen wird). Durch eine veränderbare PIN kann es vor unbefugter Benutzung geschützt werden. Mit Hilfe des SIM wird das Mobile Equipment (also üblicherweise das Mobiltelefon) einem Netz zugeordnet und authentifiziert.
SMS*	Short Message Service (englisch für Kurznachrichtendienst, Abk. SMS) ist ein Telekommunikationsdienst zur Übertragung von Textnachrichten, die meist Kurzmitteilungen oder ebenfalls SMS genannt werden. Er wurde zuerst für den GSM-Mobilfunk entwickelt und ist in verschiedenen Ländern auch im Festnetz als Festnetz-SMS verfügbar. Über SMS-Gateways können weitere Dienste angebunden werden
Updates*	Update bezeichnet die Aktualisierung von Software
USB*	Der Universal Serial Bus (USB) ist ein serielles Bussystem zur Verbindung eines Computers mit externen Geräten. Mit USB ausgestattete Geräte oder Speichermedien (USB-Speichersticks) können im laufenden Betrieb miteinander verbunden (Hot Swapping) und angeschlossene Geräte sowie deren Eigenschaften automatisch erkannt werden.
Viren*	Ein Computervirus (lateinisch virus ‚Gift‘; im Deutschen neutralen, auch maskulinen Geschlechts, Plural -viren) ist ein sich selbst verbreitendes Computerprogramm, welches sich in andere Computerprogramme einschleust und sich damit reproduziert. Die Klassifizierung als Virus bezieht sich hierbei auf die Verbreitungs- und Infektionsfunktion. Einmal gestartet, kann es vom Anwender nicht kontrollierbare Veränderungen am Status der Hardware, am Betriebssystem oder an der Software vornehmen (Schadfunktion). Computerviren können durch vom Ersteller gewünschte oder nicht gewünschte Funktionen die Computersicherheit beeinträchtigen und zählen zur Malware.
VPN*	Ihrem Ursprung nach bilden VPNs innerhalb eines öffentlichen Wählnetzes in sich geschlossene virtuelle Teilnetze. Mit einem solchen Teilnetz ist ein separates Netzwerk gemeint, welches in dem darüber liegenden Wählnetz derart eingebettet ist, dass es von den anderen Netzen nichts

mitbekommt – gerade so, als verfüge jedes VPN über seine eigene Leitung. Man kann sagen, VPN ist ein eigenständiges Netz, gekapselt in einem anderen Netz.

Wipe*	Wipe (vom englischen für „wischen“ oder „putzen“) ist eine Software, die zum sicheren Löschen von Dateien dient. Wird eine Datei mit Wipe gelöscht, so überschreibt es diese mehrmals mit Nullen, speziellen Bit-Mustern und/oder Zufallsdaten. Dadurch soll gewährleistet werden, dass die gelöschten Daten rekonstruiert werden können.
WLAN*	WLAN (Wireless Local Area Network; deutsch wörtlich „drahtloses lokales Netzwerk“ – Wireless LAN, W-LAN, WLAN) bezeichnet ein lokales Funknetz, wobei meistens ein Standard der IEEE-802.11-Familie gemeint ist. Für diese engere Bedeutung wird in manchen Ländern (z. B. USA, Großbritannien, Kanada, Niederlande, Spanien, Frankreich, Italien)