

160.2

Weisung Informationssicherheit und Datenschutz (InDaW)

vom 28. Oktober 2025

In Kraft seit: 1. Januar 2026
(nachgeführt bis 1. Januar 2026)

Inhaltsverzeichnis

1. Allgemeines.....	1
Art. 1 Zweck.....	1
Art. 2 Geltungsbereich/Nutzerverpflichtung.....	1
Art. 3 Nutzungsbeschränkung	1
2. Verantwortung	2
Art. 4 Zuständigkeiten.....	2
Art. 5 Mitarbeitende, Behörden- und Kommissionsmitglieder	2
3. Datenschutz und Informationssicherheit.....	2
Art. 6 Updates und Patching.....	2
Art. 7 Ausbildung und Sensibilisierung	3
Art. 8 Zugangs- und Zugriffsschutz	3
Art. 9 Passwörter	4
Art. 10 Weitere Identifizierungsmassnahmen.....	4
Art. 11 Virenschutz / Virenbefall	5
Art. 12 Datensicherheit, -löschung und Entsorgung.....	5
4. Hard- und Software (inkl. Telefonapparate)	6
Art. 13 Hardware	6
Art. 14 Software	6
Art. 15 Kalendereinträge.....	6
5. Nutzung von E-Mail und Internet	7
Art. 16 Allgemeine Bestimmungen	7
Art. 17 E-Mail im Besonderen.....	7
Art. 18 Private Nutzung von Internet und E-Mail	7
Art. 19 Unangemessene Benutzung.....	7
6. Einsatz mobiler Geräte, Homeoffice und Videokonferenzen	8
Art. 20 Allgemeine Bestimmungen mobiles Arbeiten	8
Art. 21 Geräte der Stadt Affoltern am Albis	8
Art. 22 Homeoffice	8
Art. 23 Videokonferenzen	9
Art. 24 Protokollierung	9
Art. 25 Sanktionen	9

7. Ergänzungen zu dieser Weisung	10
Art. 26 Kompetenzdelegation	10
8. Übergangs- und Schlussbestimmungen.....	10
Art. 27 Inkrafttreten.....	10

1. Allgemeines

Art. 1 Zweck

¹Diese Weisung regelt die Nutzung der Informations- und Kommunikationstechnologie (ICT-Infrastruktur), im Speziellen den Gebrauch von E-Mail und Internet und die Verwendung mobiler Geräte. Gegenstand der Weisung ist zudem der verantwortungsvolle Umgang mit Informationen (insbesondere Personendaten) zur Gewährleistung des Datenschutzes.

²Sie bezweckt den Schutz der Informationen vor einem Verlust der Vertraulichkeit, Verfügbarkeit und Integrität.

Art. 2 Geltungsbereich/Nutzerverpflichtung

¹Die Weisung gilt für alle fest oder temporär angestellten Mitarbeitenden sowie für die Behörden- und Kommissionsmitglieder.

²Sie gilt zudem für alle Personen, welche die IT-Infrastruktur der Politischen Gemeinde Affoltern am Albis nutzen oder auf entsprechende Inhalte zugreifen. Für Nutzerinnen und Nutzer Dritter (z. B. Schulgemeinden), für welche die Stadt Affoltern am Albis Rechenzentrumsdienstleistungen anbietet, gilt diese Weisung sinngemäss.

³Jede Nutzerin und jeder Nutzer der ICT-Infrastruktur verpflichtet sich, alle nachfolgend aufgeführten Bestimmungen einzuhalten.

⁴Die Nutzenden treten als "Vertreterinnen und Vertreter" der Stadt Affoltern am Albis auf. Sie müssen sich an die Richtlinien der Stadt, an deren Corporate Design und Corporate Identity halten.

⁵Für Mitarbeitende, welchen die ICT-Infrastruktur von Dritten zur Verfügung gestellt wird, z. B. Stadtpolizei, gelten diese Bestimmungen so weit möglich sinngemäss.

Art. 3 Nutzungsbeschränkung

¹Die von der Stadt Affoltern am Albis zur Verfügung gestellte Hard- und Software, wie Laptop, Webdienste, Telefon, WLAN, dient ausschliesslich der Erfüllung der beruflichen Aufgaben. Ausnahmen bei der Nutzung von E-Mail und Internet sind in Art. 17 enthalten.

²Auf der zur Verfügung gestellten Hardware, wie z. B. Laptop, Diensthandy, dürfen keine privaten Programme oder Apps installiert werden.

2. Verantwortung

Art. 4 Zuständigkeiten

¹Gemäss Informationssicherheitsleitlinie ist die oder der Informationssicherheitsverantwortliche (nachfolgend ISV genannt) die Abteilungsleiterin oder der Abteilungsleiter Präsidiales.

²Die oder der ISV ist zusammen mit der Leiterin oder dem Leiter ICT/Digitalisierung für die Umsetzung dieser Weisung verantwortlich.

Art. 5 Mitarbeitende, Behörden- und Kommissionsmitglieder

¹Die Mitarbeitenden sowie alle weiteren Funktionäre und Behördenmitglieder sind verpflichtet, die gesetzlichen Vorgaben, diese Weisung und andere interne Regelungen zu beachten.

²Sie sind verpflichtet, die ihnen zur Verfügung gestellten ICT-Mittel recht- und zweckmässig einzusetzen und mit den Informationen, insbesondere mit Personendaten und besonderen Personendaten, sorgfältig umzugehen.

³Die Nutzenden melden alle sicherheitsrelevanten Ereignisse, wie z. B. Fehlermeldungen, unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verfügbarkeit nicht explizit freigegebener Dienste, Verdacht auf Missbrauch der eigenen Benutzererkennung, Veränderung, Verlust oder Manipulation von Informationen umgehend der Leiterin oder dem Leiter ICT/Digitalisierung oder der oder dem ISV. Eigene Aufklärungsversuche sind strengstens untersagt, weil dabei allenfalls wertvolle Hinweise und Spuren verwischt werden oder verloren gehen können.

⁴Informationssicherheitsvorfälle (z. B. Verlust von Personendaten, unbefugte Weitergabe) sind unverzüglich der oder dem ISV zu melden. Diese oder dieser prüft den Vorfall und entscheidet über die weiteren Massnahmen, einschliesslich einer allfälligen Meldung an die zuständigen Stellen unter Berücksichtigung des übergeordneten Rechts.

3. Datenschutz und Informationssicherheit

Art. 6 Updates und Patching

¹Alle Geräte und Systeme der Stadt Affoltern am Albis (z. B. Server, Arbeitsplatzrechner, mobile Geräte, Fachapplikationen, Cloud-Dienste) müssen stets auf dem aktuellsten Stand gehalten werden.

²Sicherheitsrelevante Updates (Patches) sind unverzüglich, spätestens jedoch innerhalb der von der Herstellerfirma vorgegebenen Fristen einzuspielen. Funktionale Updates sind zeitnah vorzunehmen, sofern keine sicherheits- oder betriebsrelevanten Gründe dagegen sprechen.

³Für die Koordination und Durchführung von Updates ist der Bereich ICT/Digitalisierung bzw. die oder der Fachapplikationsverantwortliche zuständig. Mitarbeitende haben sicherzustellen, dass ihre Geräte für geplante Updates verfügbar sind (z. B. durch rechtzeitiges Anschliessen an das Netzwerk oder Belassen im eingeschalteten Zustand, soweit angeordnet).

Art. 7 Ausbildung und Sensibilisierung

¹Die Nutzerinnen und Nutzer werden regelmässig in den Themen ICT-Systeme und Datensicherheit geschult und sensibilisiert. Die oder der ISV kann Vorgaben über die Regelmässigkeit und den Inhalt erlassen.

²Für die interne Ausbildung der Fachanwendungen sind die jeweiligen Abteilungsleiterinnen und Abteilungsleiter verantwortlich.

³Für grundlegende ICT-Ausbildungen ist die Leiterin oder der Leiter ICT/Digitalisierung zuständig.

Art. 8 Zugangs- und Zugriffsschutz

¹Halten sich externe Personen (z.B. Servicetechniker/innen usw.) in den Büroräumlichkeiten auf, sind Massnahmen zu treffen, die einen unbefugten Zugang zu Informationen verhindern.

²Der Arbeitsplatz ist bei Abwesenheiten so zu hinterlassen, dass keine vertraulichen oder schutzbedürftigen Unterlagen und Datenträger offen zugänglich sind (z. B. Abschliessen von Türen und Verschiessen von Fenstern des Büros, Abschliessen weiterer Räume gemäss Anweisung des ISV, Sperren oder Herunterfahren des Laptops). Ausdrucke mit vertraulichen Informationen sind umgehend aus dem Drucker zu entfernen.

³Wird der PC-Arbeitsplatz (Laptop) nicht benutzt, so ist dieser abzuschalten, respektive nicht einzuschalten. Solange der Laptop nicht gesperrt ist, hat er unter der Aufsicht der Benutzerin oder des Benutzers zu stehen. Bei kurzen Abwesenheiten ist Unbefugten der Zugang zum System durch das Sperren des Laptops zu verwehren. Bei längeren Abwesenheiten (Abend, Wochenende etc.) ist der Laptop inkl. Peripherie wie Bildschirm und Drucker auszuschalten.

⁴Wo Sperrbildschirme von den Mitarbeitenden selbst eingerichtet werden können, sind sie zu benützen. Vom ISV angeordnete Bildschirmsperren dürfen nicht ausgeschaltet werden.

⁵Die Mitarbeitenden dürfen nur ihre persönlichen Benutzerkennungen oder die ihnen zugeteilten funktionellen Kennungen verwenden. Sie sind für die mit ihren Kennungen erfolgten Zugriffe verantwortlich.

⁶Der Verlust von Schlüsseln, Badges usw. ist umgehend der herausgebenden Stelle, z. B. Haustechnik, zu melden. Besteht der Verdacht, dass

Zugangs- oder Zugriffsberechtigungen unberechtigt durch Dritte genutzt werden, ist die oder der ISV umgehend zu informieren.

⁷Austretende Personen stellen sicher, dass alle schützenswerten Informationen (insbesondere besondere Personendaten), die ihnen zugänglich waren und die rechtmässig ausserhalb der Stadt Affoltern am Albis bearbeitet oder gespeichert wurden, unwiderruflich gelöscht (einfaches Löschen genügt nicht, der Datenträger muss formatiert werden) oder zurückgegeben werden.

Art. 9 Passwörter

¹Passwörter sind vertraulich zu behandeln. Sie sind verschlüsselt zu speichern und vor Unbefugten zu schützen. Dies gilt insbesondere, wenn Passwörter für den persönlichen Gebrauch notiert werden (beispielsweise mit einem Passwortmanager). Anderen Personen (z. B. Vorgesetzte, IT-Verantwortliche, ISV usw.) sind Passwörter unter keinen Umständen bekannt zu geben.

²Passwörter müssen mindestens acht Zeichen lang sein und sollen eine Kombination von Klein- und Grossbuchstaben, Ziffern und Sonderzeichen enthalten. Leicht zu erratende Passwörter und solche, die einen Bezug zur eigenen Person aufweisen (z.B. Name, Name von Angehörigen, Geburtsdatum usw.), sind nicht erlaubt. Geschäftlich genutzte Passwörter dürfen nicht privat verwendet werden. Passwörter sollten alle sechs Monate geändert werden. Sie sind sofort zu ändern, wenn ein Verdacht besteht, dass sie Dritten zur Kenntnis gelangt sind.

³Gruppenpasswörter werden nur vergeben, wenn dies zwingend erforderlich ist. Sie sind umgehend zu ändern, wenn sich die Zusammensetzung der Gruppe verändert. Gleiches gilt, wenn sie unautorisierten Personen bekannt geworden sind.

⁴Initialpasswörter müssen sofort geändert werden.

⁵Sofern technisch machbar wird eine Zwei-Faktor-Authentifizierung (2FA) eingerichtet.

Art. 10 Weitere Identifizierungsmassnahmen

¹Falls dies die oder der ISV für notwendig erachtet, oder übergeordnete Stellen es verlangen, können höhere Sicherheitsstandards eingeführt werden (z. B. PKI-Card, Fingerprint).

²PKI-Karten sind bei Nichtbenützung für Dritte unzugänglich aufzubewahren. Die Nutzerin oder der Nutzer haftet bei Missbrauch persönlich, falls sie oder er die Sorgfaltspflichten verletzt hat.

Art. 11 Virenschutz / Virenbefall

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

²Potentielle Virenträger sind E-Mail-Anhänge, Internetseiten sowie Datenträger von externen Stellen. 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. Deren Beilagen sollen keinesfalls geöffnet werden. In solchen Mails enthaltene Links dürfen nicht angeklickt werden.

³Wird ein Virenbefall festgestellt, ist unverzüglich die Leiterin oder der Leiter ICT/Digitalisierung per Telefon zu informieren.

Art. 12 Datensicherheit, -löschung und Entsorgung

¹Alle geschäftsrelevanten Dateien sind ausschliesslich im Geschäftsverwaltungs-System (GEVER-System) oder in den Fachapplikationen abzulegen. Für nicht geschäftsrelevante Daten steht den Nutzerinnen und Nutzern ein Laufwerk zur Verfügung.

²Externe Internet-Dienste, wie z.B. Online-Dateiablagen, Online-Kalender, Clouddienste oder E-Mail-Systeme dürfen nicht für geschäftliche Zwecke verwendet werden, solange diese nicht von der oder dem ISV freigegeben wurden.

³Die auf der ICT-Anlage der Stadt Affoltern am Albis gespeicherten Programme und Daten dürfen nicht auf externe Datenträger (Internet, E-Mail, Flashdisks etc.) übertragen werden. Ausnahmen sind vorgängig durch die Leiterin oder den Leiter ICT/Digitalisierung bewilligen zu lassen.

⁴Standardisierte Datenübertragungen und der Datenaustausch ist durch die Nutzung von Programmen und Plattformen zulässig, sofern diese von der oder dem ISV schriftlich freigegeben wurden oder diese Anwendungen durch ein Reglement oder eine Weisung legitimiert werden. Die Nutzung der kantonalen Plattform WebTransferZH ist erlaubt.

⁵Die Leiterin oder der Leiter ICT/Digitalisierung sorgt für eine regelmässige Sicherung aller geschäftsrelevanten Daten und die sichere Lagerung der dazu benötigten Archivmedien.

⁶Nicht mehr benötigte Daten müssen von Datenträgern (z.B. USB-Datenträger, Speicherkarten usw.) unwiederbringlich gelöscht werden (einfaches Löschen genügt nicht, der Datenträger muss formatiert werden, i.d.R. rechte Maustaste).

⁷Nicht mehr benötigte Informationsträger, wie Festplatten, USB-Datenträger, die vertrauliche Informationen enthalten oder einmal enthielten, sind physikalisch zu vernichten (z.B. Schreddern).

4. Hard- und Software (inkl. Telefonapparate)

Art. 13 Hardware

¹Sämtliche Hardwareanpassungen, -neuanschlüsse und -verschiebungen dürfen nur durch die Leiterin oder den Leiter ICT/Digitalisierung oder durch eine von ihm bezeichnete Person vorgenommen werden.

²Alle Hardwarekomponenten sind im Originalzustand zu belassen. Das Anbringen von Bildern, Klebeetiketten, Abziehbildern etc. ist an der gesamten Infrastruktur untersagt. Vorbehalten bleiben systembedingte Informationen, welche durch die Leiterin oder den Leiter ICT/Digitalisierung angebracht werden.

³Die Hardware (z. B. Laptop, Server, Drucker und Telefon) darf nur von ausgebildetem Personal bedient werden. Sämtliche Hardwareteile sind immer vor Sonnenlicht zu schützen und sauber zu halten.

Art. 14 Software

¹Alle Software-Installationen dürfen nur durch den Bereich ICT/Digitalisierung oder durch eine von der Leiterin oder vom Leiter ICT/Digitalisierung bezeichnete Person vorgenommen werden.

²Jegliche Software-Installation, insbesondere das Öffnen oder Herunterladen von Programmen (insbesondere Dateien mit Endung *.exe, *.vbs, *.zip, *.wav, *.mpeg, *.avi oder *.bat usw.), Spielen, Sound-Dateien, Grafiken und sonstigen sowie nicht mit der beruflichen Tätigkeit und Funktion in Verbindung stehenden Dateien ist untersagt.

³Jede Datei muss mit einem Virens Scanner vor dem ersten Gebrauch auf Viren und Würmer geprüft werden. Komprimierte Dateien (ZIP-Files usw.) müssen hierfür allenfalls unter Mitwirkung des Bereichs ICT/Digitalisierung (wegen der Gefahr, dass Viren als ZIP-Files getarnt worden sind) geöffnet werden.

⁴**Vor** der Anschaffung von Programmen bzw. der Ausgabenbewilligung oder bei einer geplanten Nutzung von Onlinediensten (z. B. Clouds, Onlinetools) sind die detaillierten Unterlagen der Leiterin oder dem Leiter ICT/Digitalisierung frühzeitig zur Prüfung vorzulegen (Sicherstellung der Kompatibilität und des Datenschutzes).

⁵Alle Programminstallation oder die Nutzung von Onlinediensten sind vorgängig von der Leiterin oder vom Leiter ICT/Digitalisierung bewilligen und koordiniert installieren zu lassen.

Art. 15 Kalendereinträge

Alle Termine während der Bürozeit sind im persönlichen Kalender des Programmes "Outlook" einzutragen. Private Termine und Termine ausserhalb der Bürozeit dürfen ebenfalls eingetragen werden. Bei richtiger Anwendung

bleibt die Privatsphäre gewahrt. Private oder vertrauliche Termine können beim Eintrag mit dem Vermerk "Privat" gekennzeichnet werden.

5. Nutzung von E-Mail und Internet

Art. 16 Allgemeine Bestimmungen

¹Das Herunterladen und Installieren von Software aus dem Internet ist nicht gestattet. Die Leiterin oder der Leiter ICT/Digitalisierung kann das Herunterladen oder die Installation solcher Dateien für dienstliche Zwecke erlauben.

²E-Mail und Internet werden für die Erfüllung dienstlicher Aufgaben nach den Grundsätzen der Wirtschaftlichkeit, der Datensicherheit und des Datenschutzes eingesetzt.

Art. 17 E-Mail im Besonderen

¹Die Anwenderin oder der Anwender muss während der Arbeitszeit die Mailbox regelmässig auf den Eingang von E-Mails kontrollieren. E-Mails sollen in der Regel innerhalb von 1 - 2 Arbeitstagen beantwortet werden.

²E-Mails mit vertraulichem Inhalt, wie z. B. Personendaten, müssen verschlüsselt versandt werden. Ist eine Verschlüsselung nicht möglich, muss eine andere Versandart gewählt werden.

³Bei längeren Absenzen ist der Abwesenheitsassistent einzuschalten. Die automatische Weiterleitung von E-Mails (z. B. bei Abwesenheiten) an nicht kommunale E-Mail-Adressen (z. B. @stadtaffoltern.ch), z. B. die eigene private Mailbox und das Freigeben der persönlichen Mailbox an eine Drittperson sind nicht erlaubt.

Art. 18 Private Nutzung von Internet und E-Mail

¹Die private Benützung von Internet und E-Mail ist als Ausnahme zu betrachten und ist auf ein minimales Mass zu beschränken.

²Die private Nutzung sozialer Netzwerke, wie z. B. Facebook, Xing, ist während der Arbeitszeit nicht erlaubt.

Art. 19 Unangemessene Benutzung

Die Nutzung von Internet und E-Mail hat die Interessen der Stadt zu wahren und rechtliche sowie operationelle Risiken auszuschliessen. Es ist insbesondere verboten, auf Material mit widerrechtlichem, urheberrechtsverletzendem, rassistischem, beleidigendem, pornografischem oder herabwürdigendem Inhalt zuzugreifen oder solches zu verbreiten.

6. Einsatz mobiler Geräte, Homeoffice und Videokonferenzen

Art. 20 Allgemeine Bestimmungen mobiles Arbeiten

Beim Einsatz mobiler Geräte sind folgende Punkte zu beachten:

- Beim Arbeiten ausserhalb der Räumlichkeiten der Stadt Affoltern am Albis ist jederzeit sicherzustellen, dass Informationen nicht durch unbefugte Personen eingesehen oder mitgehört werden können (z. B. in öffentlichen Verkehrsmitteln oder durch Familienmitglieder im Homeoffice).
- Für dienstliche Zwecke dürfen nur durch die Stadt Affoltern am Albis genehmigte Dienste und Produkte für Kommunikation und Datenaustausch verwendet werden.
- Dienstliche Unterlagen dürfen nicht zu Hause entsorgt werden, sondern sind im Büro der ordentlichen Vernichtung zuzuführen.
- Auf mobilen Geräten wie Laptops oder Smartphones ist die Speicherung von dienstlichen Daten nach Möglichkeit zu vermeiden. Wo dies dennoch erfolgt, müssen Dokumente mit vertraulichem beziehungsweise schützenswertem Inhalt verschlüsselt gespeichert und gesichert werden.
- Die Benutzerinnen und Benutzer von mobilen Arbeitsstationen sind selbst verantwortlich für die Datensicherung und die datenschutzgerechte Aufbewahrung.

Art. 21 Geräte der Stadt Affoltern am Albis

Für Geräte, welche sich im Besitz der Stadt Affoltern am Albis befinden gilt zusätzlich zu Art. 19:

- Sicherheitsmassnahmen an mobilen Geräten dürfen nicht deaktiviert werden (Firewall, Virenschutz, Betriebssystem-Manipulationen etc.).
- Mobile Arbeitsgeräte (z. B. Laptops, USB-Datenträger, Smartphones) müssen mit einem Passwort geschützt werden.
- Der Verlust eines mobilen Gerätes ist unverzüglich der Leiterin oder dem Leiter ICT/Digitalisierung zu melden. Besteht der Verdacht, dass Zugangs- oder Zugriffsberechtigungen unberechtigt durch Dritte genutzt werden oder wurden, ist die oder der ISV umgehend zu informieren.
- Die Ortungsdienste sind bei Nichtgebrauch zu deaktivieren.

Art. 22 Homeoffice

Mitarbeitende, welche im Homeoffice arbeiten, haben die Bestimmung zum Homeoffice im Personalreglement der Stadt Affoltern am Albis sowie den Leitfaden der oder des Datenschutzbeauftragten des Kantons Zürich "Regeln für das Homeoffice" zu befolgen.

Art. 23 Videokonferenzen

Kommen Videokonferenzsysteme zum Einsatz, müssen allfällig separat erlassene Vorgaben und Bestimmungen befolgt werden. Die Bestimmungen dieser Weisung gelten sinngemäss.

Art. 24 Protokollierung

¹Im Interesse und zum Schutze des Rufes der Stadt Affoltern am Albis verpflichten sich die Nutzerinnen und Nutzer, die Bestimmungen dieser Weisung vorbehaltlos zu befolgen. Das Verhalten im Internet ist nicht anonym und kann bis zur Nutzerin oder zum Nutzer zurückverfolgt werden.

²Um die Sicherheitsanforderungen der Stadt Affoltern am Albis zu gewährleisten (z. B. Schutz vor operationellen und rechtlichen Risiken, Interessen und Ruf der Stadtverwaltung), beauftragt der Stadtrat die Leiterin oder den Leiter ICT/Digitalisierung, periodisch die zeitliche und mengenmässige Benutzung sowie die angewählten Seiten des Internets ohne Vorankündigungen zu überprüfen.

³Sicherheitsrelevante Ereignisse auf Systemen der Stadt (z. B. Login-Versuche, Administratorzugriffe, Systemfehler, Malware-Vorfälle) können protokolliert werden. Diese Protokolle dienen ausschliesslich der Sicherstellung der Informationssicherheit und der Nachvollziehbarkeit von Vorfällen.

⁴Die Auswertung dieser Protokolle erfolgt durch die Leiterin oder den Leiter ICT/Digitalisierung zusammen mit der oder dem ISV (Vier-Augen-Prinzip). Die Persönlichkeitsrechte der Mitarbeitenden sind zu wahren. Eine Verwendung der Protokolle zu anderen Zwecken ist untersagt.

Art. 25 Sanktionen

¹Bei Nichtbeachtung der Auflagen erfolgt durch die Leiterin oder den Leiter ICT/Digitalisierung bzw. die oder der ISV eine Meldung mit Antrag an die Stadtschreiberin oder den Stadtschreiber. Weitere Sofortmassnahmen durch die zuständigen Stellen bleiben vorbehalten.

²Widerrechtliche, reglementwidrige oder unangemessene Benützung von Internet und E-Mail sowie jedes andere Verhalten, welche einen Verstoss gegen die Pflichten aus dem Arbeitsverhältnis oder diese ICT-Weisung darstellen, können arbeitsrechtliche Sanktionen bis hin zur fristlosen Entlassung sowie strafrechtliche Untersuchungen zur Folge haben. Im Wesentlichen gelten die Bestimmungen des Straf- und Personalrechts.

7. Ergänzungen zu dieser Weisung

Art. 26 Kompetenzdelegation

¹Wo technische Gründe dies erfordern, kann die Stadtschreiberin oder der Stadtschreiber bzw. die Leiterin oder der Leiter ICT/Digitalisierung bzw. die oder der ISV ergänzende Vorschriften erlassen, die einen integrierenden Bestandteil dieser Weisung darstellen.

²Die Abteilungsleiterin oder der Abteilungsleiter Präsidiales erlässt ein Rollen- und Berechtigungskonzept, in welchem diese Aufgabe für Fachapplikationen auch an andere Mitarbeitende delegiert werden kann.

³Die Leiterin oder der Leiter ICT kann ein Merkblatt über die ICT erlassen.

8. Übergangs- und Schlussbestimmungen

Art. 27 Inkrafttreten

Diese Weisung tritt per 1. Januar 2026 in Kraft. Sie ersetzt die ICT-Weisung vom 11. August 2015 mit allen seitherigen Änderungen.

Affoltern am Albis, 28. Oktober 2025

Namens des Stadtrates

Präsidentin	Schreiber
Eveline Fenner	Stefan Trottmann

