Schulpflege
Freiestrasse 6 – Postfach
8952 Schlieren
www.schlieren.ch
Tel. 044 738 14 60

Reglement über die Nutzung der Mittel der Informations- und Kommunikationstechnologie (IKT) der Schule Schlieren

(vom 14. Februar 2017)

SKR Nr. 14.10

I. Allgemeine Bestimmungen

Art. 1 Ziel und Zweck

Dieses Reglement regelt die Nutzung der Mittel und Dienste im Zusammenhang mit der Informations- und Kommunikationstechnologie (IKT), welche die Schule Schlieren zur Verfügung stellen, den Schutz der Informationen und deren Bearbeitung.

Als IKT-Mittel und -Dienste gelten alle Geräte, Einrichtungen und Dienstleistungen, die zur elektronischen Verarbeitung, Speicherung oder Übermittlung von Informationen dienen, z.B. Computersysteme, Peripheriegeräte, Netzwerkkomponenten, Software, E-Mail etc.

Art. 2 Geltungsbereich

Diese Weisung gilt für Mitarbeitende der Schule Schlieren und für Drittpersonen (im Folgenden zusammenfassend Benutzerinnen und Benutzer genannt), welche als Folge eines Vertragsverhältnisses Zugang zu IKT-Mitteln und Diensten der Schule Schlieren erhalten.

II. Grundsätze für die Nutzung von IKT-Mitteln

Art. 3 Allgemeines / Nutzung von IKT Mitteln

Benutzerinnen und Benutzer sind beim Gebrauch von IKT-Mitteln für den sachgemässen Umgang und die Einhaltung der Sicherheitsvorschriften verantwortlich:

- Es dürfen keine Informationen an Unberechtigte weitergegeben werden.
- Untersagt sind das absichtliche Versenden von schädlichem Code (z.B. Viren, Würmer, Trojaner, etc.) sowie der Versand von Spam und Massenmails.
- Treten Probleme im Umgang mit IKT-Mitteln auf, so ist der Service Desk (SD) des Informatikdiensts (IT) der Schule Schlieren sofort zu informieren, damit allenfalls nötige Massnahmen eingeleitet werden können.
- Bei Verdacht auf Virenbefall ist umgehend der Service Desk zu informieren.

Die IKT-Mittel der Schule Schlieren dürfen nicht missbräuchlich verwendet werden:

- Missbräuchlich ist jede Nutzung, die gegen die Rechtsordnung (insbesondere gegen Bestimmungen des Strafgesetzbuches, des Zivilgesetzbuches, des Urheberrechtes und des Fernmeldegesetzes) und gegen interne Weisungen der Schule Schlieren verstösst.
- Eine missbräuchliche Nutzung stellt eine Verletzung der personalarbeitsrechtlichen Pflichten (Personalverordnung der Stadt und der Schule Schlieren) bzw. der vertraglichen Pflichten dar. Die strafrechtliche Verantwortlichkeit bleibt vorbehalten.

Art. 4 Passwörter

Passwörter sind persönlich und dürfen nicht an einem frei zugänglichen bzw. als Klartext an einem nicht ausreichend geschützten Ort festgehalten oder weitergegeben werden.

- Beim Verdacht, dass Unberechtigte ein Passwort kennen, ist dieses umgehend zu ändern.
- Benutzerpasswörter müssen aus mindestens 8 Zeichen zusammengesetzt sein (Administratorenpasswörter mind. 12 Zeichen) und neben Gross- und Kleinbuchstaben auch Zahlen oder Sonderzeichen enthalten (mindestens drei dieser Kategorien müssen enthalten sein).
- Trivialpasswörter wie Benutzer-ID, Name, Vorname, Geburtsdatum usw. dürfen nicht verwendet werden.
- Das neue Passwort darf nicht aus dem alten Passwort ableitbar sein (Herauf- und Herunterzählen ist nicht erlaubt).
- Passwörter müssen spätestens nach 90 Tagen geändert werden.
- Nach fünf Fehlversuchen wird das betroffene Konto gesperrt. Ein gesperrtes Konto kann nur vom Service Desk wieder freigegeben werden.
- Benutzer- und Administratorenpasswörter, welche einmal verwendet wurden, dürfen erst nach 10 erfolgten Wechseln wiederholt werden.
- Im Fall eines gesperrten Kontos oder eines vergessenen Passwortes ist der Service Desk zu kontaktieren.

Art. 5 Herunterladen und installieren von Software und Mediadateien

Das Herunterladen, Speichern, Installieren und Weiterverbreiten von Software aller Art ist grundsätzlich untersagt. Das Herunterladen und Installieren von betrieblicher Software erfolgt in der Regel durch die IT. Ausnahmen sind Softwareupdates von vorgängig installierten Programmen.

Das Herunterladen von Mediendateien (Audio, Video usw.) ist nur für berufliche Zwecke gestattet.
Es darf nicht gegen Urheberrechte (Lizenzbestimmungen) verstossen werden.

Art. 6 Netzwerk

Der Anschluss von IKT-Mitteln ans Netzwerk der Schule Schlieren, welche nicht durch die IT zugelassen wurden, ist untersagt. Hierzu gehören auch Netzwerkkomponenten wie Switch, Access-Points, Router, etc.

Art. 7 Datenübertragung (ohne E-Mail)

Unter Datenübertragung versteht man das Versenden von elektronischen Informationen über Netzwerke (z.B. Ausdrucken von Daten). Für die Datenübertragung ohne E-Mail gelten die gleichen Bearbeitungsvorschriften wie für den Versand von E-Mails (vgl. Art. 20)

Art. 8 Verlust, Diebstahl und unsachgemässe Nutzung

Der Service Desk ist über den Verlust, den Diebstahl und die Beschädigung von IKT-Mitteln unverzüglich zu informieren.

Kosten für die Reparatur oder den Ersatz von IKT-Mitteln gehen zu Lasten der Benutzerin oder des Benutzers, wenn das Gerät unsachgemäss und mit mangelnder Sorgfalt benutzt oder der Verlust des Gerätes fahrlässig provoziert wird, beispielsweise durch unbeaufsichtigtes Stehenlassen im öffentlichen Raum.

Art. 9 Vernichtung und Entsorgung

Defekte IKT-Mittel sind ausschliesslich dem Service Desk zu übergeben. Dieser entscheidet über die weiteren Schritte.

Zu entsorgende IKT-Mittel sind dem Service Desk zur fachgerechten Löschung zu übergeben. In jedem Fall sind Datenträger so zu entsorgen, dass keine Rückschlüsse auf den Inhalt oder die gespeicherten Daten möglich sind.

Art. 10 Zugriff / Zugang zu Supportzwecken auf IKT-Mittel

Ein Zugriff auf IKT-Mittel oder ein Zugang zu Supportzwecken ist durch die Mitarbeitenden des Service Desk nur mit einer vorgängigen, expliziten Einwilligung der Benutzerin oder des Benutzers erlaubt.

Art. 11 Meldung von Sicherheitsvorfällen

Als Sicherheitsvorfälle gelten Ereignisse und Verstösse gegen die Weisungen und Reglemente, die effektiv einen Schaden verursacht haben oder einen solchen beinahe verursacht hätten.

Sicherheitsvorfälle sind unverzüglich der Schulleitung zu melden.

Art. 12 Private Nutzung der IKT Mittel

Die IKT-Mittel dürfen für private Zwecke verwendet werden, soweit die Nutzung nicht missbräuchlich ist. Ein Missbrauch liegt auch vor, wenn die für private Zwecke beanspruchten Ressourcen (insbesondere Arbeitszeit, Datennetzkapazität, Speicherkapazität, Verbrauchsmaterial wie z.B. Papier und Toner) nicht vernachlässigbar sind oder die Aufgabenerfüllung beeinträchtigen.

III. Nutzungsbestimmungen für einzelne IKT-Mittel

Art. 13 Notebook und Tablet-PC

Die Benutzerinnen und Benutzer tragen die Verantwortung für die mobilen Geräte; sowohl für die darauf gespeicherten Daten, als auch bezüglich Vertraulichkeit (Verhinderung der Einsicht durch unberechtigte Dritte), Integrität (Unterbindung unberechtigter Modifikationen an den Daten) und hinsichtlich Verfügbarkeit (die Originale aller Dokumente müssen in der Datenablage vorhanden sein).

Notebooks und Tablet-PCs verfügen über diverse Möglichkeiten zur drahtlosen Kommunikation (WLAN, Bluetooth usw.). Benutzerinnen und Benutzer sind angewiesen, bei Nichtgebrauch die vorhandenen Funktechnologien auszuschalten.

Art. 14 Thin- und Zero-Client

Thin- oder Zero-Client sind PC-Arbeitsstationen, welche via Datennetzwerk mit einem Server verbunden sind. Diese Geräte verfügen über keinen internen Speicher für Daten und Dokumente. Alle Programme, welche auf diesen Geräten gestartet werden, sind exklusive auf dem Server verfügbar. Für die Nutzung dieser Geräte sind Anmeldeinformationen (Konto-Namen und Passwort) erforderlich.

Das Speichern von persönlichen Daten geschieht auf einem Server im Netzwerk in einem geschützten Bereich, welcher von den Benutzerinnen und Benutzer selbst verwaltet wird.

Art. 15 Peripheriegeräte

Unter Peripheriegeräten werden alle Geräte zusammengefasst, die an PC, Ultrabooks oder Thin- oder Zero-Clients angeschlossen werden können, um Daten zu senden, zu empfangen oder auszugeben (z.B. Drucker, Scanner, Tastaturen, Mäuse, etc.).

Es dürfen nur bewilligte Peripheriegeräte eingesetzt werden. Die Beschaffung und Bereitstellung erfolgt durch die IT. Benutzerinnen und Benutzern ist es nicht erlaubt, selbst Peripheriegeräte zu installieren, zu betreiben oder Konfigurationen an bereitgestellten Geräten zu ändern. Die Installation erfolgt ausschliesslich durch den Service Desk.
Peripheriegeräte dürfen grundsätzlich nur mittels Kabel angeschlossen werden.

Art. 16 Private Geräte

Das Anschliessen und die Nutzung privater Geräte an das Netzwerk sind nur erlaubt, wenn vorgängig von der IT geprüft wurde, ob die minimalen IT-Sicherheitsanforderungen erfüllt sind:

- Die installierten Programme sind auf dem neusten Stand.
- Der Zugang zum Gerät ist mit einem Passwort geschützt.
- Aktualisierter Virenschutzprogramm und lokaler Firewall sind installiert.

Art. 17 Datenträger

Datenträger (USB-Stick, USB-Harddisk, CD, DVD, Backup-Medien etc.) dürfen unter Einhaltung folgender Vorgaben verwendet werden:

- Datenträger sind beim Transport durch eine entsprechende Verpackung vor physischer Beschädigung zu schützen.
- Alle Datenträger sind vorgängig einer Virenüberprüfung zu unterziehen.
- Datenträger sind vor unbefugtem Zugriff zu schützen.
- Datenträger dürfen nicht unbeaufsichtigt liegen gelassen werden.
- Die Speicherung dienstlicher Daten und Dokumente auf Datenträger ist nur zu Transferzwecken gestattet.

IV. Nutzungsbestimmungen für Software (Lizenzen)

Art. 18 Beschaffung von Software

Software wird von der IT beschafft. Diese prüft vor der Beschaffung die Kompatibilität mit den vorhandenen IKT-Infrastrukturen.

Ist die Nutzung der zu beschaffenden Software auf den IKT-Infrastrukturen nicht möglich, sucht die IT zusammen mit den Nutzenden der Software eine Lösung bzw. eine Alternative.

Art. 19 Eigentum von Software

Die Schule Schlieren ist Lizenznehmerin von Software und stellt diese zur Nutzung zur Verfügung. Die Software darf weder kopiert noch weitergegeben werden.

V. Nutzungsbestimmungen für E-Mails

Art. 20 Versand und Empfang von E-Mails

In vielen Belangen wird ein E-Mail heute praktisch einem Schriftstück gleichgesetzt. Berufliche Nachrichten sind mit der vorgesehenen Signatur zu versehen und über das Mail-Konto der Schule Schlieren zu versenden. Die Gestaltung der Signaturen muss der "Corporate Identity" der Schule Schlieren entsprechen.

Absenderadressen können gefälscht werden. Im Zweifelsfall ist eine telefonische Überprüfung beim angegebenen Absender vorzunehmen. Nachrichten von zweifelhafter Herkunft sind umgehend zu löschen. Nachrichten mit Beilagen von zweifelhafter Herkunft, welche beispielsweise Bildschirmschoner, ausführbare Dateien, Bilder usw. enthalten, sind umgehend zu löschen respektive nicht zu öffnen.

Umgehend zu löschen sind auch Informationen mit rassistischen, pornografischen oder anderweitig verletzenden Inhalten sowie Informationen, welche mit der beruflichen Tätigkeit in keinem Zusammenhang stehen. Benutzerinnen und Benutzer stellen sicher, dass keine Funktionen zur automatischen Öffnung oder Weiterleitung von Nachrichten an externe Adressen aktiviert sind. Die automatische Weiterleitung von Nachrichten von privaten Accounts an Adressen der Schule Schlieren und umgekehrt ist untersagt.

Art. 21 Ablage und Speichern von E-Mails

E-Mails sind wie alle übrigen Dokumente und Unterlagen Teil der beruflichen Tätigkeit und unterstehen den entsprechenden Aufbewahrungs- und Archivierungsvorschriften.

Für das Speichern der E-Mails gelten folgende Regelungen:

- Alle E-Mails in den Ordnern "Posteingang", "Gesendete Objekte" und "Gelöschte Objekte", welche älter als 60 Tage sind, werden automatisch entfernt und in einen Zwischenspeicher verschoben. Nach weiteren 60 Tagen werden sie definitiv gelöscht. Alle anderen Ordner sind von dieser Massnahme nicht betroffen.

Art. 22 Abwesenheiten, Stellvertretung, Beendigung Anstellungsverhältnis

Bei planbaren Abwesenheiten von mehr als einem Arbeitstag ist auf eingehende Nachrichten automatisch mit einem Hinweis auf die Dauer, die Bearbeitung der Nachricht und die Stellvertretung zu antworten. Die interne Weiterleitung von eingehenden Nachrichten liegt in der Verantwortung der Benutzerinnen und Benutzer.

- Die Einsichtnahme in E-Mails, welche als "privat" gekennzeichnet sind, und deren Bearbeitung ist verwehrt. Besteht kein Unterscheidungsvermerk zwischen privaten und beruflichen E-Mails, wird davon ausgegangen, dass das E-Mail beruflich ist. Im Zweifel ist die Frage mit der Mailboxinhaberin oder dem Mailboxinhaber zu klären.
- Benutzerinnen oder Benutzer müssen vor Austritt das Postfach aufräumen und dafür sorgen, dass allfällig verbliebene geschäftsrelevante Daten korrekt abgelegt werden.
- Persönliche Mailboxen werden Beendigung des Arbeitsverhältnisses unverzüglich gelöscht.

Der Notfallzugriff auf die persönliche Mailbox oder das private Laufwerk ist in Abschnitt X geregelt.

VI. Nutzungsbestimmungen für das Internet

Art. 23 Allgemeines / Nutzungsbestimmungen für das Internet

Während der Arbeitszeit steht das Internet für berufliche Zwecke zur Verfügung. Die Nutzung für private Zwecke ist unter den Bedingungen von Art. 12 zulässig, jedoch auf ein absolutes Minimum zu beschränken.

Ausserhalb der Arbeitszeit ist die private Nutzung im Rahmen der geltenden Gesetze gestattet.

Aktivitäten, welche materiellen oder immateriellen Schaden verursachen können, sind zu unterlassen.
Werden bei der Nutzung externer Dienste (ausserhalb der Schule Schlieren) Identifikationen und Passwörter benötigt, dürfen auf keinen Fall interne Login-Namen und Passwörter verwendet werden.

Art. 24 Verbotene oder gesperrte Internetseiten

Der Service Desk kann Sperrlisten und Content Filter einsetzen um bestimmte Adressen und Dienste zu sperren.

Art. 25 Umgang mit Informationen aus dem Internet

Vom Internet bezogene Informationen sind wie Informationen aus anderen Quellen, bei welchen Autor oder Absender nicht bekannt sind, auf Echtheit, Gültigkeit und Glaubwürdigkeit zu prüfen.
Urheberrechtlich geschützte Informationen oder Produkte dürfen nicht ohne ausdrückliche Erlaubnis des Urhebers oder der Urheberin verwendet werden.

Daten aus dem Internet sind immer auf Malware (Viren, Würmer, Trojaner, Bots usw.) zu prüfen.

VII. Informationsschutz

Art. 26 Allgemeines / Informationsschutz

Unterlagen, inkl. elektronischer Daten (oder Papierabzüge davon), der Schule Schlieren, welche nicht öffentlich zugänglich sind, dürfen von den Benutzerinnen und Benutzern bei einem Austritt weder mitgenommen noch weiterverwendet werden. Die Schulleitung kann auf begründeten Antrag Ausnahmen bewilligen.

Persönliche Dateiablagen werden beim Austritt bzw. nach Beendigung des Arbeitsverhältnisses gelöscht.

Die Speicherung beruflichen Unterlagen auf lokalen Speichern von PCs ist aus Gründen der Datensicherheit nicht gestattet. Die temporäre Sicherung auf lokalen Speichern von Ultrabooks oder Tablet-PC ist erlaubt.

Art. 27 Personendaten

Die Bearbeitung von Personendaten richtet sich nach dem Personalrecht und dem Gesetz über die Information und den Datenschutz (LS 170.4).

Art. 28 Datenablage

Für die Datenablage wird für jeden Benutzer und jede Benutzerin ein persönlicher Speicherplatz auf dem zentralen Speicher eingerichtet. Die Nutzenden können diesen Speicherplatz selbst verwalten.

Art. 29 Datensicherung

Die Datenablagen auf dem Server werden täglich auf ein Drittsystem gesichert. Von lokalen Festplatten auf PCs, Notebooks und Tablet-PCs wird keine Datensicherung erstellt. Benutzerinnen und Benutzer sind für die Datensicherung selber verantwortlich respektive haben dafür zu sorgen, dass die Originale gemäss Datenablage gespeichert sind.

Bei der Sicherung und Archivierung von Daten und E-Mails findet aus technischen und praktischen Gründen keine Unterscheidung zwischen privaten und geschäftlichen Informationen statt.
Für die Datensicherung ist die IT verantwortlich. Sie findet für alle Anwendungen wie folgt statt:

- Die IT erstellt täglich eine Datensicherung, welche während 4 Wochen aufbewahrt wird.
- Am Ende jedes Monats wird eine Datensicherung erstellt, welche 6 Monate aufbewahrt wird.

VIII. Cloud Dienstleistungen

Art. 30 Allgemeines / Cloud Dienstleistungen

Den Benutzer und Benutzerinnen stehen Cloud-Dienstleistungen zur Verfügung. Cloud-Dienstleistungen sind:

- Speicherplatz
- Kollaborations-Plattform.

Über deren Nutzung und den damit verbundenen Modalitäten entscheidet die Schulleitung.

Art. 31 Hoch- und Runterladen von Dateien

Die Nutzenden der Cloud sind für das Hoch- und Runterladen von Dateien selbst verantwortlich. Cloud-Speicher sind für berufliche Zwecke bestimmt. Das Speichern von persönlichen Daten in der Cloud ist nicht gestattet.

Art. 32 Löschen von Dateien

Die Daten in der Cloud werden täglich vom Betreiber der Cloud gesichert. Die Datensicherung wird jeweils einen Monat aufbewahrt und wird anschliessend unwiderruflich gelöscht.

Art. 33 Vergabe von Zugriffsberechtigungen

Die Nutzenden der Cloud können selbst Zugriffsberechtigungen auf Verzeichnisse oder Dokumente vergeben bzw. widerrufen. Sie sind selbst verantwortlich für die korrekte Zuweisung der Berechtigungen.

Art. 34 Speicherbegrenzung

Jedem Nutzenden der Cloud steht 20 GByte Speicherplatz für das Speichern von Dokumenten zur Verfügung. Die Schulleitung kann auf Antrag der IT über eine Änderung des verfügbaren Speicherplatzes entscheiden.

IX. Protokollierung (Log-Dateien)

Art. 35 Allgemeines / Protokollierung

Für die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur anfallen, gelten das Personalrecht und das Gesetz über die Information und den Datenschutz (LS 170.4).

Die IT zeichnet als Informatikleistungserbringerin der Schule Schlieren laufend Personendaten, die bei der Nutzung der elektronischen Infrastruktur anfallen auf, zur Sicherung (Backups); Aufrechterhaltung der Informations- und Dienstleistungssicherheit, Wartung, Kontrolle der Einhaltung dieses Reglements, Nachvollzug des Zugriffs auf Datensammlungen, Kostenerfassung, Bewirtschaftung der Arbeitszeit.

Bei den Aufzeichnungen kann nicht zwischen privaten und geschäftlichen Aktivitäten unterschieden werden.

Art. 36 Auswertung

Die Auswertung von Aufzeichnungen kann sowohl nicht personenbezogen wie auch personenbezogen erfolgen.

Die nicht personenbezogene Auswertung kann durch die IT für die unter Art. 35 vorgesehenen Zwecke vorgenommen werden. Dies gilt auch für die nicht namentliche personenbezogene Auswertung zur Kontrolle der Nutzung der elektronischen Infrastruktur und zur Kontrolle der Arbeitszeiten.

Die personenbezogene Auswertung, bei welcher die Ermittlung der Identität der einzelnen Benutzerinnen und Benutzer möglich ist, wird nur bei konkretem Verdacht auf Missbrauch, erwiesenem Missbrauch, zur Behebung von Störungen und zur Abwehr von konkreten Bedrohungen, zur Bereitstellung benötigter Dienstleistungen und zur Kontrolle der individuellen Arbeitszeiten durchgeführt.

Art. 37 Auswertung von namentlich personenbezogenen Daten wegen Missbrauchs oder Missbrauchsverdachts

Eine namentliche personenbezogene Auswertung bewirtschafteter oder nichtbewirtschafteter Daten von Mitarbeitenden der Schule Schlieren wegen Missbrauchs oder Missbrauchsverdachts wird auf Antrag der vorgesetzten Stelle von der Schulleitung angeordnet. Ein Missbrauch der elektronischen Infrastruktur liegt vor, wenn die Art oder das Ausmass der Nutzung die Vorgaben der Schule Schlieren oder Rechtsvorschriften verletzt.

Stimmt die betroffene Person einer solchen Auswertung nicht zu, muss die Schulpflege die Auswertung bewilligen.

Nach der technischen Auswertung übergibt die mit der Auswertung beauftragten Personen (4-Augen-Prinzip) das Ergebnis der Auswertung der Schulleitung und informiert die betroffene Person über das Ergebnis der Auswertung.

X. Notfallzugriff

Art. 38 Allgemeines / Notfallzugriff

Grundsätzlich verfügt die Schule Schlieren über keinerlei Rechte für den Zugriff auf die persönliche Mailbox (Mails, private Kalendereinträge, Aufgaben) oder das private Laufwerk der Benutzerin oder des Benutzers.

Der Notfallzugriff definiert den unverzichtbaren, dringenden Zugriff auf die persönliche Mailbox oder den persönlichen Speicherplatz auf dem Server, bei Abwesenheit, Nichterreichbarkeit oder Ableben der entsprechenden Benutzerin oder des entsprechenden Benutzers. E-Mails und Daten, welche als "privat" gekennzeichnet sind, dürfen nicht eingesehen werden. Besteht kein Unterscheidungsmerkmal zwischen privaten und beruflichen E-Mails, wird davon ausgegangen, dass ein E-Mail beruflich ist.

Der Notfallzugriff darf nur aus beruflichen Gründen erfolgen, wenn dieser verhältnismässig ist und wenn keine Stellvertretung definiert ist, beispielsweise:

- wenn auf wichtige berufliche Mails zugegriffen werden muss;
- wenn berufliche Dokumente an nicht vorgesehenen Speicherorten und für andere Berechtigte nicht zugänglich (z. B. auf dem persönlichen Laufwerk) gespeichert wurden.

Art. 39 Notfallzugriff bei Abwesenheit oder Nichterreichbarkeit der Benutzerin oder des Benutzers

1. Die Schulleitung bzw. die pädagogische Leitung oder der Linienvorgesetzte versucht, die entsprechende Benutzerin oder den entsprechenden Benutzer telefonisch zu erreichen, um das mündliche Einverständnis einzuholen.
2. Kann die Benutzerin oder der Benutzer nicht erreicht werden, erteilt die IT der Schulleitung bzw. der pädagogischen Leitung die notwendigen Rechte.
3. Unter Einhaltung des Vieraugenprinzips wird der Notfallzugriff vorgenommen und protokolliert:
    a. Konfiguration der Delegation (automatische Abwesenheitsmeldung unter Nennung der Stellvertretung bei eingehenden E-Mails einrichten).
    b. Weiterleiten des/der benötigten Mails an die vorgesehene Stellvertretung oder Verschieben an einen regelkonformen Speicherort.
    c. Verschieben der Dokumente an den regelkonformen Speicherort.
4. Rückmeldung an die IT und die betroffene Benutzerin oder den betroffenen Benutzer, dass der Notfallzugriff ausgeführt wurde.
5. Die IT entfernt die unter Punkt 2 erteilten Zugriffsberechtigungen.

Art. 40 Notfallzugriff bei Ableben der Benutzerin oder des Benutzers

Die Benutzerin oder der Benutzer erteilt mit dem Akzeptieren der Anstellungsverfügung die Einwilligung, dass bei ihrem oder seinem Ableben auf die persönliche Mailbox und das persönliche Laufwerk zugegriffen werden darf (aus geschäftlichen Gründen).

1. Die IT erteilt im Auftrag der Schulleitung bzw. der pädagogischen Leitung die notwendigen Rechte.
2. Unter Einhaltung des Vieraugenprinzips wird der Notfallzugriff vorgenommen und protokolliert:
    a. Weiterleiten des/der benötigten Mails an die vorgesehene Stellvertretung oder Verschieben an einen regelkonformen Speicherort.
    b. Verschieben der Dokumente an den regelkonformen Speicherort.
3. Rückmeldung an die IT, dass der Notfallzugriff ausgeführt wurde.
4. Die IT löscht die persönliche Mailbox und die Daten auf dem persönlichen Laufwerk.

XI. Schlussbestimmungen

Art. 41 Inkrafttreten

Dieses Reglement tritt für das Personal der Schule Reitmen auf den 1. August 2017 in Kraft. Für das Personal der übrigen Schulen in Schlieren tritt das Reglement schulweise in Kraft, sobald die jeweilige Schule dem neuen IKT Konzept unterstellt ist.

Genehmigt mit Schulpflegebeschluss vom: 14. Februar 2017

SCHULPFLEGE Schlieren

Präsidentin: Dr. Bea Krebs

Abteilungsleiterin Bildung und Jugend: Andrea Fus

Inhaltsverzeichnis Seite