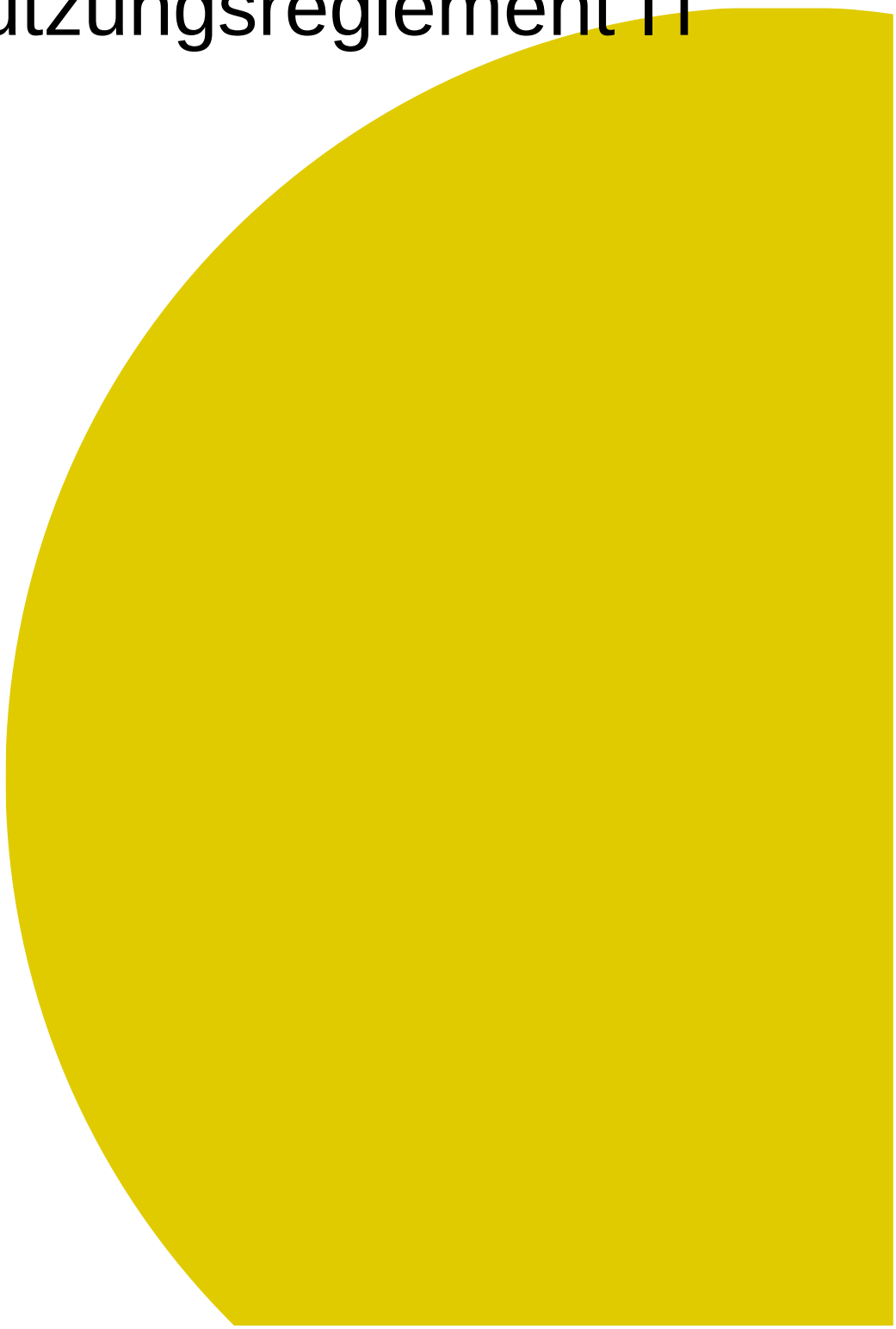
formidabel
sozialpädagogische
Schule

Nutzungsreglement IT



formidabel
sozialpädagogische
Schule

Inhaltsverzeichnis

Kantonsstrasse 30
6102 Malters
041 499 62 00
info@formidabel.ch

formidabel
sozialpädagogische
Schule

1. Zweck, Definition und Geltungsbereich

1.1 Zweck

Dieses Reglement regelt die Nutzung von Informatik-Mitteln und Informationen der sozialpädagogischen Schule formidabel. Es bezweckt den sicheren und wirtschaftlichen Einsatz der Informatik-Mittel und den Schutz der bei der Benutzung anfallenden Daten und Informationen, sowie der Persönlichkeitsrechte der Mitarbeitenden, der Lernenden und von Dritten.

Der Grund ist, dass ein unsachgemässer Gebrauch von Informatik-Mitteln die sozialpädagogische Schule formidabel unterschiedlichen Risiken aussetzen kann, wie Computer-Viren, Beeinträchtigung der Verfügbarkeit von Systemen und sogar rechtliche Konsequenzen.

1.2 Definitionen

- Hardware: PC, Laptop, Tablet, Mobile
- Software: Programme, Systeme, Applikationen
- Benutzer*in / Mitarbeitende: Angestellte der sozialpädagogischen Schule formidabel

1.3 Geltungsbereich

Dieses Reglement ist eine Ergänzung zum Arbeitsvertrag und gilt für alle Mitarbeitenden der sozialpädagogischen Schule formidabel.

Das Reglement ist gestützt auf:
- Anstellungsreglement
- Datenschutzgesetz

2. Grundsätze und Verantwortlichkeiten

Die User der Informatik-Mittel achten auf:
- den schonenden Umgang mit den zur Verfügung gestellten Ressourcen
- die Einhaltung des Reglements
- die Einhaltung der geltenden Sicherheitsvorschriften, sowie Datenschutz- und Informationsschutzanforderungen
- die Einhaltung sonstiger anwendbarer Vorschriften und gesetzlicher Bestimmungen

2.1 Verantwortung übernehmen

Die Mitarbeitenden können unabhängig von ihrer Funktion zu mehr Sicherheit beitragen, indem jede*r seine persönliche Verantwortung ernst nimmt und…

- … Regelungen, sowie mitgeltende Reglemente und Sicherheitsvorschriften kennt und einhaltet.
- … die bewusste und sichere Anwendung von Computern und Diensten und wirksame Passwörter wählt.
- … Schwachstellen meldet: Beim Auftreten von kritischen Vorfällen oder Entdecken von Schwachstellen muss umgehend eine Meldung an den internen technischen Support erfolgt. Erkannte oder vermutete Schwachstellen dürfen niemals selbst ausgetestet werden!
- … Arbeitskolleg*innen auf erkannte Sicherheitsrisiken aufmerksam macht.
- … Datenlecks und falsche Zugriffsberechtigungen proaktiv meldet.

2.2 Massnahmen der Institution

Die sozialpädagogische Schule formidabel kann zur Vermeidung von Funktionsstörungen und Missbräuchen technische Schutzmassnahmen anwenden. Sie behält sich vor, jederzeit bestimmte Funktionalitäten oder Nutzungsmöglichkeiten einzuschränken.

3. Eigentumsverhältnisse und Sorgfaltspflicht

Alle zur Verfügung gestellte Hardware sind Eigentum der sozialpädagogischen Schule formidabel. Jede*r Benutzer*in ist zum sorgfältigen Umgang mit den Geräten verpflichtet. Die Kosten für Verlust oder selbstverschuldete Defekte können, den Mitarbeitenden in Rechnung gestellt werden. Sämtliche Daten, die im Zusammenhang mit der beruflichen Tätigkeit erstellt, bearbeitet und gespeichert werden, sind ebenfalls Eigentum der sozialpädagogischen Schule formidabel.

4. Umgang mit Hardware

4.1 Private Hardware

Es ist ausdrücklich verboten, private Geräte, wie PCs oder Notebooks, bei der sozialpädagogischen Schule formidabel zu verwenden. Ausgenommen von dieser Regelung sind:

- Benutzer*innen, welche eine schriftliche Bewilligung für den Betrieb ihrer privaten Geräte erhalten haben.

- Nutzer des Gast-WLANs.
- Die E-Mail- und Kalender-Synchronisation mit privaten Smartphones und Tablets ist erlaubt. Die Nutzer akzeptieren explizit, dass bei der Synchronisation Sicherheitsrichtlinien automatisch auf den Geräten konfiguriert werden.
- Private Smartphones dürfen über das Netzwerk auf das Internet zugreifen. Die private Nutzung ist jedoch nur in den Pausen zulässig.

4.2 Beschaffung und Installation von Geräten und Software

Jegliche Hardware, welche für schulische oder geschäftliche Zwecke genutzt wird, ist über die Steuergruppe IT zu beschaffen und zu installieren.

4.3 Benutzung und Rückgabe der Geräte

Die Verwendung der zur Verfügung gestellten Hardware für private Zwecke ist grundsätzlich nicht erlaubt. Ausnahmen müssen von der Bereichsleitung Dienstleistung bewilligt werden. Notebook, Tablet, Smartphones, etc. dürfen nur durch Mitarbeitende der sozialpädagogischen Schule formidabel benutzt werden. Die Benutzung durch andere Personen ist untersagt!
Ein allfälliger Diebstahl muss unverzüglich der vorgesetzten Person und dem internen technischen Support gemeldet werden. Bei Auflösung des Arbeitsverhältnisses sind die Geräte samt Zubehör unaufgefordert dem internen technischen Support zu retournieren.

4.4 Hardwarestörungen

Alle Störungen an Geräten müssen umgehend dem internen technischen Support gemeldet werden.

4.5 Pflege und Reinigung der Geräte

Für die äusserliche Pflege und Reinigung der Geräte sind die Benutzer selbst verantwortlich. Wichtig: Bildschirme dürfen nicht mit Desinfektionsmittel gereinigt werden, da sie dadurch beschädigt werden. Gut gepflegte Hardware lebt länger und ist weniger anfällig auf Störungen. Dabei gilt: Getränke und Esswaren gehören in sichere Entfernung zu Tastatur und Geräten.

5. Umgang mit Hardware

Jegliche Software und Dienste sind über den internen technischen Support zu beschaffen und zu installieren. Das gilt auch für Freeware (kostenlos frei erhältliche Software), Open-Source Produkte (kostenlos frei erhältlicher Quellcode) oder Cloud-Dienste. Die eingesetzte Software muss ausnahmslos lizenziert sein. Zudem muss sichergestellt werden, dass die installierte Software nicht unrechtmässig kopiert wird. Private Software zu installieren ist verboten. Es ist

verboten, Programme selbst zu installieren oder vom Internet herunterzuladen (durch den internen technischen Support bewilligte Ausnahmen vorbehalten).

6. Umgang mit Kommunikationsmitteln

6.1 Allgemeine Regeln

Die gelegentliche Nutzung des Internets, E-Mail und Telefon zu privaten Zwecken ist erlaubt. Die Nutzung ist auf kurze Sequenzen zu beschränken (Bsp. Fixierung Arzttermin) und darf die betrieblichen Abläufe und Anforderungen nicht tangieren.

Folgende Handlungen sind explizit verboten:
- Hacking
- Vorsätzliches Einbringen von Schadsoftware (Viren, Trojaner, etc.)
- Verbreitung oder Konsum von pornografischen, extremistischen oder rassistischen Inhalten
- Anbieten oder Verkauf von illegalen Gütern
- Fälschen von E-Mail-Header und / oder Absender Adressen
- Erstellen oder Weiterleiten von SPAM, Kettenbriefen oder ähnlichem

6.2 Nutzung Internet

- Die sozialpädagogische Schule formidabel stellt allen Mitarbeitenden mit Zugang zu Geräten den Zugriff auf das Internet zu schulischen und geschäftlichen Zwecken zur Verfügung.
- Die Mitarbeitenden sind für ihr Handeln selbst verantwortlich. Der Zugriff auf das Internet wird mit einem Webfilter eingeschränkt; als Folge stehen nicht alle Dienste im Internet zur Verfügung. Verbotene Inhalte und solche, die der Schule schaden können, sind bestmöglich gesperrt.
- Einschränkungen durch den Webfilter sind verbindlich und dürfen nicht umgangen werden.
- Das Herunterladen von gesetzlich verbotenem Material (insbesondere pornografische Darstellungen, extrem-politisches Material u.Ä.), sowie Verletzungen des Copyrights können für den Benutzer strafrechtliche Konsequenzen haben.
- Die Benutzer anerkennen mit dem Gebrauch des Internets ausdrücklich das Recht der sozialpädagogischen Schule formidabel, auf Basis der gesetzlichen Grundlagen Datenverkehr aufzuzeichnen und im Rahmen des Datenschutzgesetzes auszuwerten.

6.3 Nutzung Social Media

Grundsätze
- Im Namen der sozialpädagogischen Schule formidabel dürfen nur durch die Geschäftsleitung autorisierte Sprecher Inhalte veröffentlichen, kommentieren oder in anderer Form zugänglich machen.

- Wir veröffentlichen auf keinen Fall vertrauliche Informationen über unsere Schule.
- Wir verfassen keine beleidigenden, diskriminierenden, rassistischen, sexistischen und vulgären Beiträge.
- Wir beteiligen uns nie an Hetzkampagnen oder sonstigen Diskussionen oder Handlungen, die der sozialpädagogischen Schule formidabel schaden können.

Social Media in der Freizeit
Beteiligen wir uns ausserhalb der Arbeitszeit als Privatperson an einer Diskussion, die die sozialpädagogische Schule formidabel oder ihre Angebote betrifft, betonen wir, dass es sich dabei um unsere persönliche Meinung handelt. Wenn wir auf ein Thema stossen, von welchem wir der Meinung sind, dass unsere Schule als Institution auf Social Media auftreten oder eingreifen müsste, melden wir dies dem/der Kommunikationsverantwortlichen oder der Geschäftsleitung.

6.4 Nutzung E-Mail / Outlook

6.4.1 Sicherheit

- Die Überwachung des geschäftlichen, wie auch des privaten E-Mailverkehrs erfolgt im Rahmen der entsprechenden gesetzlichen Bestimmungen und Weisungen.
- E-Mails unbekannter oder fragwürdiger Herkunft sollten sofort gelöscht werden. Auf keinen Fall unbekannte oder nicht erwünschte, angehängte Dateien öffnen. Im Zweifelsfall ist vor dem Öffnen eines fragwürdigen Anhangs der interne technische Support zu kontaktieren.
- Kreditkartennummern, Passwörter, Geheimcodes, sensible und personenbezogene Daten u.Ä. sind ausdrücklich nicht unverschlüsselt via E-Mail zu versenden.
- Verdächtige Emails / Anhänge dürfen nicht geöffnet werden. Im Zweifel vor dem Öffnen den internen technischen Support anfragen.
- Informationen, dass verdächtige E-Mails von einem formidabel-Account verschickt werden, müssen zwingend und unverzüglich dem internen technischen Support gemeldet werden.

6.4.2 E-Mail

Die nachfolgenden Punkte sind für Mitarbeitende der sozialpädagogischen Schule formidabel, wenn immer möglich, im internen und externen Mailverkehr, zu beachten:

- Notwendigkeit: E-Mails sind nicht immer das ideale Kommunikationsmittel. E-Mails sind insbesondere ungeeignet für Diskussionen, persönliche Kritik oder vertrauliche Themen.
- Es ist anzustreben, dass die Bearbeitung von E-Mails in der Regel innerhalb von 2 Arbeitstagen erfolgt. Kann ein Anliegen nicht innerhalb von dieser Zeit befriedigend beantwortet werden, wird eine kurze Info an die entsprechende Person geschickt.
- Betreff: knappe und eindeutige Formulierung wählen, welche auf den Inhalt des E-Mail schliessen lässt.
- Signatur: vollständige Signatur gemäss Vorgaben ist in der Kommunikation mit Dritten / Externen immer zu verwenden.
- Form: es gelten die gleichen Grundsätze wie im Briefverkehr (Schriftsprache, Rechtschreibung, Anrede etc.).

- Verwendung CC-Funktion: Nur diejenigen Benutzer ins CC nehmen, für welche der Inhalt informativ relevant ist. Unnötige CC vermeiden und E-Mails nicht unnötig weiterleiten.
- Verwendung des Verteilers «alle» ist nicht erlaubt. Informationen an alle können über das Infomail verbreitet werden. Ausnahmen können durch den Geschäftsleiter erteilt werden.
- Verwendung BCC-Funktion: Mit dieser Funktion kann eine E-Mail für andere Empfänger nicht erkennbar versteckt an weitere Personen mitgesendet werden. Die Funktion ist standardmässig ausgeblendet und darf nur in Ausnahmefällen verwendet werden.
- Gemeinsame interne zu bearbeitende Dokumente sollen über Teams genutzt oder als Link in der E-Mail eingebettet werden. Anhänge sollten vermieden werden.
- Abwesenheitsmeldung: bei einer Abwesenheit von 2 Arbeitstagen oder mehr wird eine Abwesenheitsmeldung gemäss Vorgaben aufgeschaltet.
- E-Mails sollen, wenn immer möglich zu den regulären Arbeitszeiten verschickt werden. Wochenende und Ferien sind Erholungszeiten und sollen, wenn immer möglich entsprechend respektiert und eingehalten werden.
- Die Nutzung vom Email für private Zwecke ist untersagt.

6.4.3 Kalender

Mit diesem Nutzungsreglement wird die Open-Calendar-Policy eingeführt.

Neuer Standard: Die Kalenderberechtigung wird für alle Mitarbeitenden standardmässig auf «Eingeschränkte Details» angepasst. Das heisst, dass folgende Angaben für jeden in der sozialpädagogischen Schule formidabel sichtbar sind:

- Betreff des Termins
- Ort des Termins
- Zeitraum des Termins

Nicht sichtbar sind nach wie vor:

- Teilnehmende des Termins (ausser man ist selbst Teilnehmer)
- Details im Termin (Text und Anhänge)
- Als «Privat» gekennzeichnete Termine

Vorteile dieser Anpassung:

- Fördert die Vertrauenskultur
- Zeitersparnis beim Finden von gemeinsamen Terminen
- Kein Teilen von Kalendern mehr notwendig

Private Termine: Vertrauliche Termine (z.B. HR-Termine) , sowie private Termine (z.B. Arztbesuche etc.) sollten konsequent als privat markiert werden. Das Markieren von Terminen als Privat, um die Open-Calender-Policy zu umgehen, soll unterlassen werden.

Terminart: Es soll darauf geachtet werden, die Terminart dem Termin entsprechend korrekt auszuwählen

- Frei: insbesondere Termine, welche rein informativ im eigenen Kalender erscheinen (z.B. Ferien der Teamkollegen, Geburtstage etc.)

- Gebucht: Meetings vor Ort oder ausser Haus (wichtig: bei Meetings ausser Haus Anfahrtszeit im Kalender ebenfalls einplanen)
- Abwesend: nach Belieben z.B. für Meetings ausser Haus oder private Termine ausser Haus
- An einem anderen Ort tätig: insbesondere zu verwenden, wenn man sich im Homeoffice befindet

6.5 Nutzung Geschäftstelefon

- Die sozialpädagogische Schule formidabel stellt einzelnen Mitarbeitenden ein Mobiltelefon zur Verfügung, damit diese ihre Kommunikationsaufgaben besser, schneller, rationeller und zeitgemäss erfüllen können.
- Die Mitarbeitenden sind wie bei allen anderen Arbeitsgeräten und Arbeitshilfen zur sachgerechten und sorgfältigen Behandlung verpflichtet. Bei Verlust muss die SIM-Karte unverzüglich gesperrt werden und der Verlust ist sofort zu melden. Defekte Geräte sind der Bereichsleitung DL zu melden. Die Kosten für Verlust oder selbstverschuldete Defekte übernimmt der Verursacher.
- Wir machen alle Mitarbeitenden darauf aufmerksam, dass das Telefonieren während der Fahrt mit dem Handy am Ohr verboten ist!
- Die Nutzungslimits und Regeln zum Privatgebrauch von geschäftlichen Mobiltelefonen sind im Spesenreglement festgehalten.
- Bei Arbeiten im Homeoffice ist zwingend die Rufumleitung auf das Mobiltelefon zu aktivieren.

Ausstattung
Bestellungen von Mobiltelefonen und das zur Verfügung gestellte Zubehör, Sperrungen im Verlustfall und Reparaturaufträge dürfen nur durch die Bereichsleitung DL vorgenommen werden. Sie ist auch für die Festlegung der Gerätemarke und Typen verantwortlich.
Spezielles Zubehör muss von den Mitarbeitenden selbst beschafft und bezahlt werden.

6.6 Nutzung Drucker

- Im Rahmen unserer Umweltpolitik sind Ausdrucke auf ein Minimum zu reduzieren. Es dürfen nur Sachen ausgedruckt werden, die wirklich benötigt werden.
- Standardmässig ist der Schwarz-Weiss-Druck eingestellt. Es darf nur in Ausnahmefällen farbig ausgedruckt werden. Dadurch können unnötige Kosten gespart werden (ein Farbdruck kostet 5x mehr als ein Schwarz-Weiss-Druck).
- Drucken und kopieren für den privaten Gebrauch ist gegen Gebühr erlaubt.

7. Umgang mit Daten, sowie Datenschutz und Sicherheit

Die Rechte an geschäftlichen und schulischen Daten stehen der sozialpädagogischen Schule formidabel zu. Auf diese Daten haben Zugriff:

- die Nutzenden selbst

- die zuständige vorgesetzte Person
- soweit vorhanden, eine Stellvertretung des Nutzenden

7.1 Umgang mit Daten

Es ist sehr wichtig, mit den uns anvertrauten Informationen sorgfältig umzugehen. Nicht nur, weil uns das Datenschutzgesetz und andere Vorschriften dazu verpflichtet, sondern vor allem, weil uns der Persönlichkeitsschutz der Mitarbeitenden und Lernenden am Herzen liegt. Dabei spielt es keine Rolle, ob die Daten auf dem Papier stehen oder im Computer gespeichert sind. In diesem Zusammenhang sind folgende Punkte einzuhalten:

7.1.1 Datenbearbeitung

Mit dem Benutzerkonto erhalten die Mitarbeitenden Zugang zu vertrauenswürdigen und sensiblen Daten. Die Einsicht, Bearbeitung und Speicherung dieser Daten ist ausschliesslich für Geschäftszwecke unabhängig des Ortes des Zugriffs (Büro oder Fernzugriff) zulässig. Die Einsicht, Bearbeitung und Speicherung von Daten sind ausschliesslich mit Geräten der sozialpädagogischen Schule formidabel erlaubt. Eine Ausnahme besteht für die Synchronisation von E-Mail- und Outlook Daten. Mitarbeitende, welche die Daten-Synchronisation in Anspruch nehmen, willigen ein, dass die Löschung des betroffenen Gerätes bei Bedarf möglich ist. Die Verantwortung für eine ordnungsgemässe Bearbeitung der Geschäftsdaten liegt immer beim Mitarbeitenden.

Offizielle Pdf-Dateien aus e-Case und iFound dürfen durch Mitarbeitende nicht nachbearbeitet werden.

7.1.2 Umgang mit vertraulichen Informationen

Papiere und andere Datenträger mit vertraulichen Informationen sollten nicht länger als nötig herumliegen und nach Gebrauch weggeschlossen werden. Jegliche Schüler- und Personendaten fallen unter diesen Grundsatz.

7.1.3 Datensicherheit

- In Sitzungszimmer wie auch am Arbeitsplatz dürfen weder Arbeitspapiere noch jegliche Angaben auf Flipcharts und Whiteboards zurückgelassen werden.
- Daten sicher entsorgen: vertrauliche Dokumente müssen im Aktenvernichter verkleinert werden. Datenträger dürfen nicht selbst gelöscht werden, dazu muss der technische Support kontaktiert werden, welcher das fachgerecht erledigt. Normal gelöschte Daten sind mit wenig Aufwand rekonstruierbar.

7.1.4 Speichern von Daten / Laufwerke

- Ordner auf dem Fileserver werden durch den technischen Support gemäss Berechtigungen erstellt und die Benutzer entsprechend berechtigt.

- Es dürfen keine Daten lokal auf dem PC oder Notebook dauerhaft abgelegt werden. Die Ablage erfolgt auf den zentralen Systemen. Dort ist sichergestellt, dass die hohen Anforderungen bezüglich Datenschutzes und Datensicherheit korrekt umgesetzt werden.
- Es ist nicht gestattet, private Daten (Fotos, Filme, Musik etc.) auf der Infrastruktur der Schule zu speichern.

7.1.5 Umgang mit Daten bei Austritt

- Beim Austritt eines / einer Mitarbeitenden werden die Accounts gesperrt.
- Aus Datenschutzgründen darf die sozialpädagogische Schule formidabel ohne ausdrückliche, schriftliche Einwilligung des / der ausgetretenen Mitarbeitenden nachträglich nicht mehr auf die Accounts zugreifen.
- Die Accounts sowie alle damit assoziierten Daten werden 3 Monate nach Austritt des / der Mitarbeitenden endgültig gelöscht.

7.2 Datenschutz und IT-Sicherheit

7.2.1 Persönliches Benutzerkonto

Die persönliche Benutzererkennung darf nur von dem / der Mitarbeitenden selbst genutzt werden. Es ist verboten, andere Personen unter seiner / ihrer persönlichen Benutzererkennung arbeiten zu lassen, wie auch selbst fremde Benutzerkonten zu benutzen. Bei einer Vermutung, dass das eigene Konto und das zugehörige Passwort von Dritten missbraucht wurde, muss sofort das Passwort geändert werden und umgehen eine Meldung an den technischen Support erfolgen.

7.2.2 PC oder Notebook sperren

Auch für kürzere Absenzen muss das Arbeitsgerät (PC oder Notebook) gesperrt werden, indem eine Abmeldung erfolgt, der die Bildschirmsperre aktiviert. Dies ist ein wirksamer Schutz vor Missbrauch des eigenen Benutzerkontos.

7.2.3 Passwort

7.2.3.1 Der richtige Umgang mit dem Passwort

- Das zum Benutzerkonto gehörende Passwort ist persönlich und darf ausser dem / der Mitarbeitenden niemand kennen. Das Passwort darf niemals weitergegeben werden. Auch Vorgesetzte, technischer Support und IT Supporter haben keinen Grund, das Passwort zu kennen, auch wenn jemand danach fragt.
- Die Weitergabe von Passwörtern, sowie die Verwendung von gemeinsamen Passwörtern ist untersagt
- Das Passwort muss in regelmässigen Abständen gewechselt werden. Es soll jedes Mal eine völlig neue Kombination gewählt werden. Das Passwort sollte sich nicht auf den / die Mitarbeitende selbst, die Abteilung oder Funktion beziehen.

- Bei der Eingabe des Passwortes sollte der Benutzer / die Benutzerin unbeobachtet sein. Ist dies nicht möglich, muss das Passwort möglichst bald geändert werden.
- Passwörter dürfen nicht auf Zettel geschrieben werden, welche von Dritten eingesehen werden können.

7.2.3.2 Ein wirksames Passwort wählen

Grundsatz
Ein Passwort wählen, das einfach zu behalten, aber schwierig zu erraten ist. Dabei gilt es, die folgenden Regeln zu berücksichtigen:

- Muss mindestens 8 Ziffern lang sein
- Muss mindestens Gross- und Kleinbuchstaben enthalten
- Muss mindestens ein Satz- oder Sonderzeichen wie «!», «#» enthalten
- Muss mindestens eine Zahl enthalten
- Die letzten 5 Passwörter dürfen nicht verwendet werden

7.2.4 Remote Access-Zugang (VPN-Zugang)

Remote Access wird verwendet, wenn von ausserhalb des formidabel-Netzwerkes auf die formidabel-Umgebung zugegriffen werden soll. Dies z.B. im Homeoffice über das private WLAN. Remote Access ist ausschliesslich mit 2-Faktor Authentifizierung möglich. Die 2-Faktor Authentifizierung wird per privatem Smartphone mit der Microsoft Authenticator APP durchgeführt. Der technische Support stellt dafür eine entsprechende Lösung zur Verfügung.

7.2.5 Betrügerische Datenerschleichung

Wirtschaftsspione, Hacker und andere Personen geben sich oft als jemand anderes aus, um sich durch geschickte Fragen nach internen Telefonnummern, Namen von Mitarbeitenden, Passwörtern oder ähnlichen Informationen Zugang zu unseren Systemen zu verschaffen. Dieses Vorgehen – Social Hacking genannt – umgeht alle technischen Sicherheitsvorkehrungen und zielt auf das schwächste Glied in der Sicherheitskette: den Menschen. Deshalb muss zwingend beachtet werden:

- Misstrauisch sein: Bei unbekannten Fragestellern muss die Identität zwingend überprüft werden und der / die Vorgesetzte informiert werden. Anfragen betreffend Auskunft über die Institution oder Mitarbeitende müssen immer schriftlich angefordert werden.
- Vorsicht wahren: Bei Anfragen, nicht gestattete Dinge zu tun, beispielsweise Informationen oder Passwörter weiterzugeben, Zugang zu gewähren etc., ist umgehend der / die Vorgesetzte zu informieren und der Anfrage nicht stattzugeben. Niemand hat das Recht, nach dem Passwort zu fragen und ebenso ist niemand darauf angewiesen, das Passwort zu kennen.
- Verdächtige Vorfälle sind sofort dem / der Vorgesetzten und dem technischen Support zu melden.

8 Überwachungsregelungen

8.1 Aufzeichnung von Daten über die Nutzung

Die sozialpädagogische Schule formidabel oder die beauftragten Informatik-Leistungserbringer zeichnen im Hinblick auf die Aufrechterhaltung des Betriebes, zur Gewährleistung der Dienstleistungsqualität, zur Einhaltung der Reglemente oder zur Ermittlung und Behebung von Betriebsstörungen oder Missbräuchen laufend Daten über die Nutzung der ICT-Mittel inklusive Datum und Uhrzeit auf. Dies sind:

- Verkehrsranddaten von Kommunikationsvorgängen
- Protokollierung über Datei-Zugriffe/-mutationen/-löschungen in entsprechenden Protokoll-Dateien (Logfiles).
- Telefonnummern
- Protokolle des Internetzugangs und E-Mail-Verkehrs und das Volumen der transportierten Daten

8.2 Überwachung Infrastruktur

Die sozialpädagogische Schule formidabel hat aus Sicherheitsgründen auf allen Komponenten (Server, Laufwerke, Netzwerk) eine Überwachungssoftware installiert, um allfällige Auffälligkeiten sofort überprüfen zu können und auf Unregelmässigkeiten sofort reagieren zu können.

Die Daten von Punkt 8.1 und 8.2 werden nur für die notwendige Zeitspanne aufgezeichnet und anschliessend gelöscht.

9 Vorgehen bei Missbrauch

- Die Einhaltung dieser Nutzungsreglungen kann bei Verdacht überprüft werden. Nach Rücksprache mit der vorgesetzten Person können mit Vorankündigung für eine bestimmte Zeitspanne personenbezogene Auswertungen in Bezug auf Missbräuche vorgenommen werden. Die Daten werden nur für die notwendige Zeitspanne aufgezeichnet und anschliessend gelöscht. Missbrauch liegt vor, wenn Bestimmungen der Nutzungsreglungen missachtet werden oder gegen arbeitsrechtliche Treuepflichten verstossen wird. Werden tatsächlich wiederholte oder schwere Verstösse gegen dieses Nutzungsreglement festgestellt, ist mit Sanktionen von der Verwarnung bis zur fristlosen Entlassung zu rechnen. Schadenersatzansprüche bleiben ausdrücklich vorbehalten. Straftaten im Zusammenhang mit Kinderpornographie, Rassenhetze, etc. werden angezeigt.
- Kann nach erfolgter personenbezogener Auswertung ein Missbrauch einem bestimmten Mitarbeitenden zugeordnet werden, informiert die Datenschutzbeauftragte die vorgesetzte Stelle des betreffenden Mitarbeiters und die Geschäftsleitung.

- Die Geschäftsleitung entscheidet aufgrund der festgestellten Verletzung der arbeitsrechtlichen Pflichten über das weitere Vorgehen. Missbräuche haben in erster Linie arbeitsrechtliche Konsequenzen.
- Ferner können für die betreffenden Nutzenden die Nutzungsmöglichkeiten für ICT-Mittel eingeschränkt und / oder ICT-Mittel entzogen werden.
- Missbräuchliche, insbesondere rechtswidrige Daten können blockiert oder gelöscht werden.
- Bei Verdacht auf eine Straftat hält sich die sozialpädagogische Schule formidabel vor, eine Anzeige zu erstatten.

10 Schlussbestimmungen

10.1 Verstösse gegen das Reglement

Das vorliegende Nutzungsreglement ist für alle Mitarbeitenden der sozialpädagogischen Schule formidabel verbindlich. Verstösse dagegen stellen Vertrags- resp. Weisungsverletzungen dar, werden geahndet und können demnach disziplinarische Massnahmen bis hin zur fristlosen Auflösung des Anstellungsverhältnisses zur Folge haben.

10.2 Änderungen und Aufhebung des Reglements

Das Reglement kann bei Vorliegen veränderter Verhältnisse ganz oder teilweise geändert oder vollständig aufgehoben werden, ohne dass für Mitarbeitende ein Anspruch auf ein gleiches oder ähnliches System entsteht. Beschlossene Änderungen werden den Mitarbeitenden schriftlich bekannt gegeben.

10.3 Inkrafttreten

Das vorliegende Nutzungsreglement tritt per 1. Januar 2023 in Kraft.

Für die Bestätigung dieses Nutzungsreglements unterschreibt der Mitarbeiter ein separates Dokument.

iFound Nr.: 3.2.1. - 004
Verfasst durch: Sabine Winiger
Freigabedatum: 06. April 2023