primarschule
dielsdorf

Weisung zur Informationssicherheit

Verabschiedet durch die Primarschulpflege am:	15.04.2024
In Kraft gesetzt per:	16.04.2024

Inhaltsverzeichnis

1 Allgemeine Bestimmungen 3
1.1 Gegenstand und Zweck 3
1.2 Geltungsbereich 3
1.3 Grundlagen 3
2 Verantwortung 3
2.1 Informationssicherheitsverantwortlicher 3
2.2 Mitarbeitende sowie weitere Funktionäre und Behördenmitglieder 3
3 Datenschutz und Informationssicherheit 3
3.1 Zugangs- und Zugriffsschutz 3
3.2 Passwörter 4
3.3 Datensicherung, -löschung und Entsorgung von Informationsträgern 4
3.4 Virenschutz 4
3.5 Hard- und Software 4
4 Nutzung von E-Mail und Internet 4
5 Private Nutzung von IT-Mitteln 5
6 Einsatz mobiler Geräte 5
7 Ausnahmen 5

Primarschule Dielsdorf, Postfach, 8157 Dielsdorf Telefon 044 853 23 35 E-Mail primarschule@psdielsdorf.ch www.primarschule-dielsdorf.ch

1 Allgemeine Bestimmungen

1.1 Gegenstand und Zweck

Diese Weisung regelt die Nutzung der Informations- und Kommunikationstechnologie (IT-Mittel), 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). Sie bezweckt den Schutz der Informationen vor einem Verlust der Vertraulichkeit, Verfügbarkeit und Integrität.

1.2 Geltungsbereich

Die Weisung gilt für alle fest oder temporär angestellten Mitarbeitenden sowie für die Behörden- und Kommissionsmitglieder der Primarschule Dielsdorf, welche die IT-Infrastruktur (Software und/oder Hardware) der Primarschule nutzen.

1.3 Grundlagen

Die rechtlichen Grundlagen der Primarschule Dielsdorf sind:

- Gesetz über die Information und den Datenschutz (IDG, Ordnungsnummer 170.4)
- Verordnung über die Information und den Datenschutz (IDV, Ordnungsnummer 170.41)
- Verordnung über die Informationsverwaltung und -sicherheit (IVSV, Ordnungsnummer 170.8)
- Personalverordnung
- Vollzugsverordnung zur Personalverordnung
- Weitere interne Weisungen

Weiter sind datenschutzrechtliche Bestimmungen in den verschiedenen Spezialgesetzen und -verordnungen (insbesondere im Personalrecht) zu beachten.

Grundlage dieser Weisung bildet zudem die Leitlinie zur Informationssicherheit.

2 Verantwortung

2.1 Informationssicherheitsverantwortlicher

Informationssicherheitsverantwortlicher der Primarschule Dielsdorf (nachfolgend ISV) entspricht dem Ressortvorstand Präsidium. Der ISV ist für die Umsetzung dieser Weisung verantwortlich und ist Ansprechstelle für Fragen und für sicherheitsrelevante Vorkommnisse. Er ist befugt, sämtlichen Nutzern Weisungen bezüglich Informationssicherheit zu erteilen.

2.2 Mitarbeitende sowie weitere Funktionäre und Behördenmitglieder

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

Sie sind verpflichtet die ihnen zur Verfügung gestellten IT-Mittel recht- und zweckmässig einzusetzen und mit den Informationen, insbesondere Personendaten und besondere Personendaten, sorgfältig umzugehen. Die Mitarbeitenden melden alle sicherheitsrelevanten Ereignisse (Probleme, Vorfälle, Mängel usw.) sowie Schäden und Verlust von Hardware und Software umgehend dem ISV.

3 Datenschutz und Informationssicherheit

3.1 Zugangs- und Zugriffsschutz

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

Der Arbeitsplatz ist bei Abwesenheiten so zu hinterlassen, dass keine vertraulichen oder schutzbedürftigen Unterlagen und Datenträger offen zugänglich sind (Abschliessen von Türen, Abschliessen weiterer Räume gemäss Anweisung des ISV, Sperren oder Herunterfahren der PCs/Laptops, Einschliessen der Laptops nach Arbeitsschluss). Ausdrucke mit vertraulichen Informationen sind umgehend aus dem Drucker zu entfernen. Wo Bildschirmsperren von den Mitarbeitenden selbst eingerichtet werden können, sind sie zu benutzen.

Die Mitarbeitenden dürfen nur ihre persönlichen Benutzererkennungen oder die ihnen zugeteilten funktionellen Kennungen verwenden. Sie sind für die mit ihren Kennungen erfolgten Zugriffe verantwortlich. Der Zugriff auf Personendaten, die nicht zur Aufgabenerfüllung benötigt werden, ist nicht erlaubt.

Primarschule Dielsdorf, Postfach, 8157 Dielsdorf Telefon 044 853 23 35 E-Mail primarschule@psdielsdorf.ch www.primarschule-dielsdorf.ch

Der Verlust von Hardware, Schlüsseln, Badges, Chipkarten usw. ist umgehend dem ISV zu melden. Besteht der Verdacht, dass Zugangs- oder Zugriffsberechtigungen unberechtigt durch Dritte genutzt werden, ist der ISV umgehend zu informieren.

Austretende Personen (Angestellte sowie Behörden- und Kommissionsmitglieder) stellen sicher, dass alle schützenswerten Informationen (insbesondere Personendaten), die ihnen zugänglich waren und die ausserhalb der Primarschule Dielsdorf bearbeitet oder gespeichert wurden, unwiderruflich gelöscht (einfaches Löschen genügt nicht) oder zurückgegeben wurden.

3.2 Passwörter

Passwörter 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). Andere Personen (zum Beispiel Vorgesetzen, IT-Verantwortlichen, ISV, usw.) sind Passwörter unter keinen Umständen bekannt zu geben.

Passwörter müssen mindestens aus acht Zeichen bestehen 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. Dienstlich genutzte Passwörter dürfen nicht privat verwendet werden. Passwörter sollten regelmässig gewechselt werden. Sie sind sofort zu ändern, wenn ein Verdacht besteht, dass sie Dritten zur Kenntnis gelangt sind. Ein früher benutztes Passwort darf nicht mehr gewählt werden.

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

3.3 Datensicherung, -löschung und Entsorgung von Informationsträgern

Schulrelevante administrative Daten müssen zentral auf einem Laufwerk gespeichert werden. Der ISV sorgt für eine regelmässige Sicherung aller relevanten Daten und die sichere Lagerung der dazu benötigten Archivmedien.

Nicht mehr benötigte Daten müssen von Datenträgern (z.B. USB-Datenträger, Speicherkarten usw.) unwiederbringlich gelöscht werden (einfaches Löschen genügt nicht). Nicht mehr benötigte Informationsträger (z.B. USB-Datenträger, CD-ROM usw.), die vertrauliche Informationen enthalten oder einmal enthielten, sind physisch zu vernichten (z.B. Schreddern).

3.4 Virenschutz

Die Mitarbeitenden dürfen die Sicherheitssoftware (Virenschutz, Firewall usw.) nicht ausschalten, blockieren oder ihre Konfiguration verändern. E-Mails mit unbekanntem Absender, verdächtigem Betreff oder unüblichem Inhalt sind vorsichtig zu behandeln, da sie von der Virenschutzsoftware nicht erkannte Viren enthalten könnten. Ihre Anhänge sowie Linds auf Websiten sollen keinesfalls geöffnet werden. Jeder Verdacht auf Virenbefall muss sofort dem ISV gemeldet werden.

3.5 Hard- und Software

Bei der Installation oder beim Anschluss von Software- und Hardware-Erweiterungen (insbesondere Kommunikationseinrichtungen und externe Massenspeicher) ist besondere Vorsicht walten zu lassen. Nur der IT-Verantwortliche darf Geräte in die Reparatur oder zur Entsorgung geben. Er stellt sicher, dass keine schützenswerten Daten auf diesem Weg die Amtsstelle verlassen.

Änderungen an den Systemeinstellungen (Installation, Deinstallation, Änderung der Konfiguration usw.) dürfen nur durch die zuständige Stelle [IT- Verantwortliche] vorgenommen werden. Neuanschaffungen von Hardware und Software müssen immer in Absprache mit dem IT-Verantwortlichen erfolgen.

4 Nutzung von E-Mail und Internet

- E-Mail und Internet werden für die Erfüllung dienstlicher Aufgaben nach den Grundsätzen der Wirtschaftlichkeit, der Datensicherheit und des Datenschutzes eingesetzt.
- Der Besuch von Internet-Seiten und der Versand von E-Mails mit Inhalten, die als diskriminierend, beleidigend oder verletzen aufgefasst werden können, sind generell untersagt.

- Ebenso untersagt ist der Versand von geschäftlichen oder privaten E-Mails, die gegen die Rechtsordnung (z.B. Strafrecht, Datenschutz) bzw. die Rechte Dritter (z.B. Urheberrechte, Lizenzrechte, Persönlichkeitsrechte) verstossen.
- An eine E-Mail angehängte Dateien, die von einer unbekannten, seltsamen oder nicht vertrauenswürdigen Quelle stammen, dürfen unter keinen Umständen geöffnet werden. Solche E-Mails sind umgehend zu löschen; anschliessend ist der Outlook-Papierkorb zu leeren.
- Internet-Dateien dürfen nicht aus unbekannten, nicht vertrauenswürdigen oder seltsamen Quellen heruntergeladen werden.
- Bei Verdacht auf Verletzung der vorangehenden Bestimmungen oder wenn konkrete Anhaltspunkte für einen Missbrauch oder für Risikoverhalten hinsichtlich Datensicherheit vorliegen, ist die [ ] berechtigt, den betreffenden individuellen elektronischen Verkehr für eine beschränkte Zeit zu überwachen.
- Der Internetverkehr wird über ein Webfiltermodul auf schädliche Inhalte geprüft. Zudem sind standardisiere Webfiltermodule aktiviert, die z.B. Nudity-, Criminal Activities-, Extemistic Sites-, Drugs-, Games / Gables- und Weapons-Kategorien blocken.

5 Private Nutzung von IT-Mitteln

Die zurückhaltende Benutzung von IT-Mitteln für private Zwecke ist grundsätzlich gestattet, soweit dadurch die Systemressourcen wie Speicher und Übertragungskapazität nicht im Übermass belastet werden. Die private Nutzung soll möglichst ausserhalb der Arbeitszeit erfolgen und kann von der vorgesetzten Stelle verboten werden. Während der Arbeitszeit ist sie auf ein Minimum zu beschränken.

6 Einsatz mobiler Geräte

Beim Einsatz mobiler Geräte sind folgende Punkte zu beachten:

- Auf mobilen Geräten (z.B. Notebooks, USB-Datenträger, Smartphones usw.) müssen Dokumente mit vertraulichem beziehungsweise schützenswertem Inhalt verschlüsselt gespeichert werden.
- Mobile Arbeitsgeräte müssen mit einem Boot-Passwort geschützt werden.
- Die Benutzerinnen und Benutzer von mobilen Arbeitsstationen sind selbst für die Datensicherung und die datenschutzgerechte Aufbewahrung verantwortlich.
- Mobile Geräte dürfen in öffentlich zugänglichen Räumen nicht unbeaufsichtigt gelassen werden.
- Die Geräte dürfen nicht Dritten zur Nutzung überlassen werden.
- Der Verlust eines mobilen Gerätes ist unverzüglich dem ISV zu melden.
- Es dürfen keine zusätzlichen Applikationen installiert werden. Besteht ein begründeter Bedarf, ist die Genehmigung des ISV einzuholen.
- Eine Verbindung zu drahtlosen Netzwerken (z.B. WLAN) ist nur zulässig, wenn eine Verschlüsselung (Zugang mit Passwort) eingesetzt wird.
- Die Benutzung wird in der Nutzungsvereinbarung, welche bei Übernahme des iPads unterzeichnet wird, abschliessend geregelt.

7 Ausnahmen

Der ISV entscheidet über Ausnahmen von der vorliegenden Weisung. Entsprechende Gesuche sind ihm mit Begründung per E-Mail einzureichen.

Diese Weisung wurde von der Primarschulpflege erlassen und per 16.04.2024 in Kraft gesetzt.

PRIMARSCHULPFLEGE DIELSDORF

Der Präsident	Die Schulverwalterin
M. Baumgartner	S. Takacs

Primarschule Dielsdorf, Postfach, 8157 Dielsdorf Telefon 044 853 23 35 E-Mail primarschule@psdielsdorf.ch www.primarschule-dielsdorf.ch