Konzept

Informationssicherheit und Datenschutz

Schulpflegebeschluss Nr. 173-13/19 vom 18. November und 165-14/19 vom 16. Dezember 2019

Inhaltsverzeichnis

1 Einleitung

Die Primarschule Wettswil ist für ihre Aufgabenerfüllung von zuverlässig funktionierenden Systemen der Informations- und Kommunikationstechnologie abhängig. Zur Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit, Nachvollziehbarkeit und Authentizität der Informationen und deren Verarbeitungssysteme nach § 7 Gesetz über die Information und den Datenschutz (IDG, LS 170.4) verabschiedet die Schulpflege das vorliegende Konzept. Es trägt zum Datenschutz und zur Informationssicherheit bei, indem es das von der Primarschule Wettswil angestrebte Informationssicherheitsniveau, die Informationssicherheitsziele sowie die geeigneten Massnahmen definiert. Weiter beinhaltet dieses Konzept eine Beschreibung der Informationssicherheitsorganisation, des Schutzbedarfs, der Berechtigungs- und Zugriffsdefinitionen sowie der Informationssicherheitsmassnahmen.

2 Geltungsbereich

Das Konzept Informationssicherheit und Datenschutz bezieht sich sowohl auf elektronische wie auch nicht elektronisch gespeicherte Daten. Es gilt für alle Mitarbeitenden und Schülerinnen und Schüler (SuS) der Primarschule Wettswil. Bei Vertragspartnern, die Daten bearbeiten, muss sichergestellt werden, dass die im Folgenden aufgeführten Anforderungen eingehalten werden.

3 Informationssicherheitsniveau

Das Informationssicherheitsniveau der Primarschule Wettswil entspricht der Sicherheitsstufe 2 (von 3) nach § 8 Abs. 2 Informatiksicherheitsverordnung (ISV). Diese Einstufung erfolgt aufgrund der Tatsache, dass die Anzahl der betroffenen Personen gering ist, alle wesentlichen Funktionen und Aufgaben durch IT- und Netzwerksysteme unterstützt werden und ein Ausfall von IT- und Netzwerksystemen die Aufgabenerfüllung nicht beeinträchtigen darf. Ausserdem bearbeitet die Primarschule Wettswil auch Daten, die einen erhöhten Schutz vor unberechtigten Zugriffen und unerlaubten Änderungen benötigen.

4 Informationssicherheitsziele

Aus der Einstufung ergeben sich die folgenden Informationssicherheitsziele nach § 7 IDG:

Integrität	Informationen müssen richtig und vollständig sein.
Nachvollziehbarkeit	Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.
Verantwortung	Die Mitarbeitenden der Schule sind sich ihrer Verantwortung beim Umgang mit Informationen, IT-Systemen und Anwendungen bewusst. Sie unterstützen die Informationssicherheitsziele.
Verfügbarkeit	Informationen müssen bei Bedarf vorhanden sein. Die Ausfallzeiten dürfen keine wesentlichen Auswirkungen auf den Schulbetrieb haben.
Vertraulichkeit	Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen.
Zurechenbarkeit	Informationsbearbeitungen müssen einer Person zugerechnet werden können.

5 Informationssicherheitsorganisation

Die Schulpflege, der Informationssicherheitsverantwortliche[1] und der Anwendungs- und Datenverantwortliche sowie die operativen Leiter der einzelnen Bereiche haben die zentralen Rollen in der Informationssicherheitsorganisation inne (Abb. 1).

Die Informationssicherheitsorganisation ermöglicht es der Primarschule Wettswil, das angestrebte Informationssicherheitsniveau zu erreichen und dieses aufrechtzuerhalten. Informierte und geschulte Mitarbeitende sind die Voraussetzung dafür, dass die Primarschule Wettswil die gesteckten Informationssicherheitsziele erreichen kann. Auf ihre Sensibilisierung und Weiterbildung ist besonderes Gewicht zu legen.

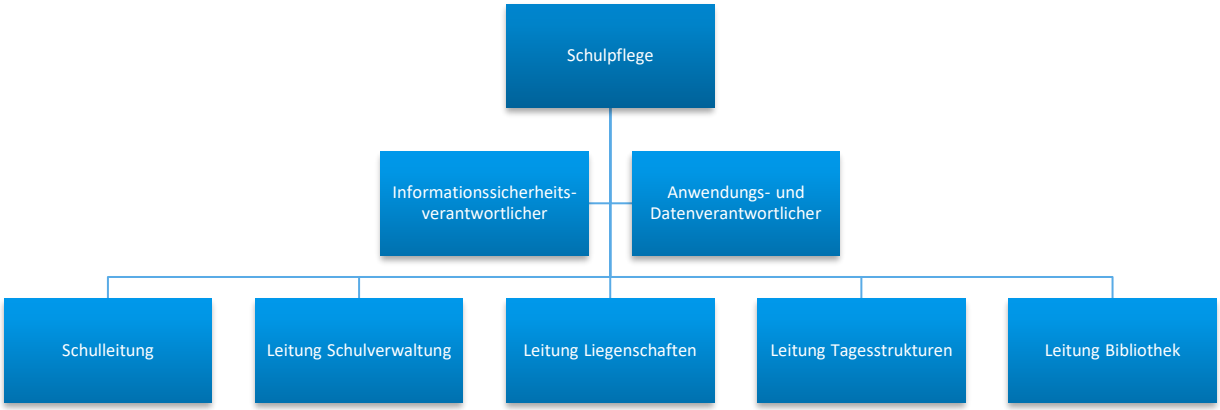

Abb. 1: Organigramm Informationssicherheitsorganisation der Primarschule Wettswil

5.1 Schulpflege

Der Datenschutz und die Informationssicherheit sind für alle Bereiche, in denen personenbezogene Daten verarbeitet werden, von grundlegender Bedeutung. Die Schulpflege trägt die Gesamtverantwortung für die Informationssicherheit und den Datenschutz in der Primarschule Wettswil. Sie legt das Konzept Informationssicherheit und Datenschutz fest und genehmigt die für die Informationssicherheit erforderlichen Massnahmen und Mittel.

Sie weist die Rollen *Informationssicherheitsverantwortlicher* und *Anwendungs- und Datenverantwortlicher* bestimmten Personen zu.

5.2 Informationssicherheitsverantwortlicher

Zur Umsetzung der Informationssicherheitsziele und Überwachung der Einhaltung des angestrebten Sicherheitsniveaus wird durch die Schulpflege eine Person bestimmt, die für die Informationssicherheit verantwortlich ist. In der Regel ist dies der Leiter des Ressorts Informatik und selbst Mitglied der Schulpflege. Er ist für die Ausarbeitung und Nachführung des Konzepts Informationssicherheit und Datenschutz verantwortlich, entscheidet über sicherheitsrelevante Fragen und berichtet in dieser Funktion direkt der Schulpflege. Er ist die Anlaufstelle für Hinweise auf Schwachstellen und verfügt über ein angemessenes Wissen sowie entsprechende Fähigkeiten.

Die Aufgaben des Informationssicherheitsverantwortlichen umfassen im Einzelnen:

[1] Auf die weiblichen Formen wird im Folgenden zugunsten der Lesbarkeit verzichtet.

- Erstellung, Überarbeitung und Überprüfung des Konzepts Informationssicherheit und Datenschutz sowie daraus hervorgehender Sicherheitsvorgaben (Weisungen, Merkblätter, usw.)
- Kontrolle des Fortschritts der Umsetzung von Informationssicherheitsmassnahmen
- Bericht an die Schulpflege über den Stand der Informationssicherheit und des Datenschutzes sowie über zu treffende Informationssicherheitsmassnahmen und Herbeiführung einer Entscheidung
- Beratung der Mitarbeitenden und der Schulpflege in Belangen der Informationssicherheit und des Datenschutzes
- Bindeglied zum kantonalen Datenschutzbeauftragten
- Planung und Anordnung von Sensibilisierungs- und Schulungsmassnahmen zum Thema Informationssicherheit

5.3 Anwendungs- und Datenverantwortlicher

Für alle Prozesse, Daten, Anwendungen, IT- und Netzwerksysteme benennt die Schulpflege eine verantwortliche Person als Anwendungs- und Datenverantwortlichen, der den jeweiligen Schutzbedarf (Klassifizierung) bestimmt und die Zugriffsberechtigungen vergibt. Er stellt sicher, dass der Zugriff auf Informationssysteme zur Nutzung, Administration und Wartung nur durch Berechtigte erfolgt.

Die Aufgaben des Anwendungs- und Datenverantwortlichen umfassen:

- Kontrolle der Erfüllung des Konzepts Informationssicherheit und Datenschutz
- Führung des Inventars über die Schutzobjekte (Daten, Anwendungen, IT-Systeme, Dossiers) in Zusammenarbeit mit den operativen Leitern
- Klassifizierung der Daten in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit
- Aktualisierung der Berechtigungsgruppen (siehe Kap. 6.3)
- Zuteilung der Zugriffsberechtigungen und Anpassung der Zugriffs (siehe Kap. 6.4)
- Regelmässige Überprüfung der Zugriffsmatrizen auf Richtigkeit und Zweckmässigkeit (in Zusammenarbeit mit operativen Leitern und Informationssicherheitsverantwortlichem) sowie bei Bedarf Vornahme von Korrekturmassnahmen
- Erstellung von Ausnahmebewilligungen in Rücksprache mit dem Informationssicherheitsverantwortlichen
- Zurücksetzung der Passwörter
- Erstellung, Überarbeitung und Kontrolle der Massnahmen für die Informationssicherheit und den Datenschutz
- Erstellung von Notfallplänen für längere Ausfälle
- Verantwortung für die Archivierung oder Vernichtung von Daten
- Ansprechperson für Betroffene in Sachen Datenschutz (Auskunfts- und Löschbegehren)

5.4 Operative Leiter

Die operativen Leiter der einzelnen Bereiche unterstützen den Informationssicherheitsverantwortlichen in seiner Tätigkeit durch die frühzeitige Beachtung sicherheitsrelevanter Aspekte in allen Alltagsgeschäften und Projekten. Sie unterstützen den Anwendungs- und Datenverantwortlichen, indem sie die Verantwortung für die Anwendungen und Daten ihrer Bereiche übernehmen.

Die Aufgaben der operativen Leiter im Hinblick auf Informationssicherheit und Datenschutz umfassen:

- Kontrolle der Erfüllung der Datenschutz- und Informationssicherheitsbestimmungen
- Verantwortung für den sicheren Betrieb der in der Verantwortung des operativen Leiters liegenden Anwendungen in Bezug auf Vertraulichkeit und Integrität der Datensammlungen sowie Verfügbarkeit der Anwendungen und Datensammlungen

- Koordination und Umsetzung von Sensibilisierungs- und Schulungsmassnahmen zum Thema Informationssicherheit
- Informationsstelle für die in ihrem Verantwortungsbereich liegenden Anwendungen und Datensammlungen
- Verantwortung für die Bearbeitung (inklusive Bekannt- und Weitergabe) oder Vernichtung der in seinem Verantwortungsbereich liegenden Daten

6 Schutzbedarf und Zugriffsberechtigungen

Für alle Fachanwendungen und Informationen muss festgelegt werden, wer für ihre Sicherheit verantwortlich ist. Zudem ist zu definieren, wie hoch der Schutzbedarf in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit ist.

Für die Zugriffskontrolle werden die Mitarbeitenden und SuS in Berechtigungsgruppen eingeteilt. Für jede Gruppe wird bestimmt, welche Zugriffsberechtigungen sie auf die Informationen, Anwendungen und Systeme hat.

6.1 Schutzbedarfskategorien

Die an der Primarschule Wettswil verarbeiteten Informationen lassen sich in Hinblick auf Persönlichkeitsverletzungen in drei Kategorien einteilen.

Kategorie	**Beschreibung**
Sachdaten	Informationen, die sich nicht auf Personen beziehen
Personendaten	Informationen, die sich auf bestimmte oder bestimmbare Personen beziehen wie Vorname, Name, Adresse
Besondere Personendaten	Information, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht.

6.2 Zugriffskontrolle

Alle zu schützenden Dokumente in Papierform wie auch alle elektronisch gespeicherten Daten sind durch Zugriffskontrolle vor unerlaubter Nutzung zu schützen. Dies gilt insbesondere auch für alle eingesetzten IT-Systeme (Server, Endbenutzergeräte, Netzwerke) und Anwendungen (Office365, Schulportal, E-Mail, Scolaris, Lehreroffice etc.). Jeder Anwendende wird mindestens durch eine Identifikation und ein Passwort gegenüber dem System identifiziert und authentifiziert. Bezüglich Zugriffs auf Informationen wird unterschieden zwischen: Kein Zugriff, Lesen, Bearbeiten und Löschen.

IT-Systeme, Netzwerkkomponenten und die Abtrennung des internen Netzwerks von Fremdnetzen (Firewall) werden von einem externen Auftragnehmenden unterhalten. Dieser dokumentiert die Schule mit den notwendigen Unterlagen (Grundsätze, Filterregeln mit zugelassenen Verbindungen, Empfängerkreis und Periodizität der Auswertungen und Meldungen). Für Supportaufgaben kann der Auftragnehmende auf alle Systeme zugreifen.

6.3 Berechtigungsgruppen

Die Mitarbeitenden und Schülerinnen und Schüler der Schule Wettswil werden in Berechtigungsgruppen unterteilt. Diese Unterteilung dient der Übersicht über Berechtigungsstrukturen. Die Zuordnung

der Personen zu den Berechtigungsgruppen erfolgt durch den Anwendungs- und Datenverantwortlichen und wird als separate Liste geführt.

Folgende Berechtigungsgruppen werden an der Primarschule Wettswil definiert:

Berechtigungsgruppe	**Beschreibung**
Administratoren	Personen, die Hardware oder Software administrieren. In der Regel erhalten nicht alle dieser Gruppe zugeordneten Personen die Administratorenrechte für eine Hardware oder Software, sondern bestimmte Einzelpersonen dieser Gruppe.
Schulverwaltung	Leitung der Schulverwaltung sowie alle Mitarbeitenden der Schulverwaltung
Schulleitung	Alle Schulleiter
Leitung Tagesstrukturen	Leiter der Tagesstrukturen
Leitung Bibliothek	Leiter der Bibliothek
Leitung Liegenschaften	Leiter der Liegenschaften
Schulpflege	Alle Schulpflegemitglieder
Lehrpersonen	Alle Lehrpersonen, schulische Heilpädagogen, Therapeuten
ICT-Verantwortliche	Alle Mitglieder der Informatikkommission
MA Tagesstrukturen	Alle Mitarbeitenden des Bereichs Tagesstrukturen (inkl. Leitung)
MA Bibliothek	Alle Mitarbeitenden der Bibliothek (inkl. Leitung)
MA Liegenschaften	Alle Mitarbeitenden im Bereich Liegenschaften (inkl. Leitung)
Mitarbeitende	Alle Mitarbeitenden der Schule Wettswil
SuS	Alle Schüler und Schülerinnen der Schule Wettswil

6.4 Zugriffsmatrizen

Für die Zuweisung von Zugriffsrechten werden drei Fälle unterschieden:

1) Zugriff auf Daten via Dateisystem (Server, Cloud)
2) Zugriff auf nicht elektronisch gespeicherte Daten
3) Zugriff auf Anwendungen
4) Zugriff auf eingesetzte IT-Systeme (Server, Endbenutzergeräte, Netzwerke)

Für jede Zugriffsart wird eine Zugriffsmatrix erstellt. Im Fall 1) wird für jedes Verzeichnis festgehalten, welche Berechtigungsgruppen darauf und gegebenenfalls auf dessen Unterverzeichnisse Zugriff haben und welche Art von Zugriff erlaubt ist. Ebenfalls wird im Fall 2) für jede Dokumentenart festgehalten, wo sich die Dokumente befinden und wer darauf zugreifen darf. Im Fall **Fehler! Verweisquelle konnte n icht gefunden werden.** werden alle Anwendungen, die für den Schulbetrieb relevant sind (ohne Lernsoftware), identifiziert und es wird festgelegt, wer diese Anwendungen benutzen darf. Im Fall 4)

wird für jedes IT-System eine Beschreibung aufgeführt. Zudem wird erfasst, welche Funktionen durch welche Berechtigungsgruppe durchgeführt werden darf.

In den Zugriffsmatrizen kann durchaus der Fall auftreten, dass die Zugriffsberechtigung nicht allen Personen einer Berechtigungsgruppe gewährt wird, sondern nur einzelnen Personen einer Gruppe.

Der Anwendungs- und Datenverantwortliche verwaltet die Zugriffsmatrizen und ist für deren Aktualisierung verantwortlich. Er darf Ausnahmen für den Zugriff gewähren, muss Aufträge hierfür aber schriftlich formulieren und vom Empfänger visieren lassen sowie die Durchführung dem Empfänger schriftlich bestätigen. Zudem sorgt er für die korrekte und vollständige Ablage der Aufträge zwecks Nachvollziehbarkeit.

7 Informationssicherheitsmassnahmen

Die folgenden Massnahmen sollen die Informationssicherheit gewähren. Der Informationssicherheitsverantwortliche ist generell für die Einhaltung dieser Massnahmen verantwortlich. Für jede Massnahme ist jedoch definiert, durch wen oder wodurch sie sichergestellt werden soll. Werden Dienstleistungen durch externe Auftragnehmende erbracht, ist die Schule dafür verantwortlich, dass die erforderlichen Sicherheitsmassnahmen umgesetzt werden.

7.1 Informationssicherheitsorganisation

Name	Beschreibung	Zeitpunkt	Verantwortung
Organisation	Das Organigramm Informationssicherheitsorganisation regelt alle Funktionen sowie deren Stellvertretung. Durch ausreichende Dokumentation und Instruktion wird sichergestellt, dass die Stellvertretenden ihre Aufgabe erfüllen können.	Immer	Informationssicherheitsverantwortlicher Anwendungs- und Datenverantwortlicher
Outsourcing	Bei der Auslagerung von Datenbearbeitungen werden der Datenschutz und die Datensicherheit gewährleistet, indem schriftliche Verträge abgeschlossen und entsprechende Kontrollmassnahmen vereinbart werden.	Nach Bedarf	Informationssicherheitsverantwortlicher
Eintritt und Austritt von Mitarbeitenden	Der beim Eintritt oder Austritt von Mitarbeitenden durchlaufene Prozess beinhaltet die Information über das Konzept Informationssicherheit und Datenschutz. Neueintretende unterzeichnen eine Nutzungsvereinbarung. Bei Austritt bestätigt der Austretende mit seiner Unterschrift, dass alle schuli-	Immer	Operative Leiter

	schen Daten auf persönlichen Geräten (inkl. Backups) gelöscht wurden.		
Sensibilisierung	Mindestens einmal jährlich informieren die operativen Leiter die Mitarbeitenden über die Informationssicherheit, den Datenschutz, aktuelle Gefahren und zu treffende Massnahmen.	Jährlich	Alle
Weisungen	Die Mitarbeitenden werden angewiesen, die Gesetze sowie die vertraglichen Regelungen und internen Richtlinien einzuhalten. Sie unterstützen durch eine sicherheitsbewusste Arbeitsweise die Sicherheitsmassnahmen. Informationssicherheitsfragen und Hinweise auf Schwachstellen werden an die für die Informationssicherheit verantwortliche Person gerichtet. Die Lehrpersonen instruieren die SuS betreffend Informationssicherheit.	Immer	Alle

7.2 IT-Systeme

Aus der Definition der Informationssicherheitsziele ergeben sich folgende Massnahmen:

Name	Beschreibung	Zeitpunkt	Verantwortung
IT-Systeme	Die IT-Systeme werden nach der Beschaffung sicher installiert (gemäss anerkannten Sicherheitsstandards) und betrieben, mittels eines Änderungsmanagements verwaltet und in einem geregelten Prozess ausser Betrieb genommen.	Nach Bedarf	Externer IT-Support, operative Leitungen
Archivierung / Löschung	Alle Daten werden gemäss den regulatorischen Vorgaben archiviert. Falls eine Aufbewahrung nicht mehr erforderlich ist, werden diese sicher gelöscht, beziehungsweise vernichtet.	Jährlich	Schulverwaltung operative Leitungen Externer Archivar
Aktualisierungen/ Updates	Alle IT-Systeme und Anwendungen werden regelmässig aktualisiert und mit den aktuellsten Sicherheitsupdates versorgt.	wöchentlich	Externer IT-Support

Mobile Geräte / Software	Der Einsatz von Arbeitsplatzrechnern und mobilen Geräten inklusive der Verwendung von privaten Geräten (Bring Your Own Device) sowie die Installation von Software auf Arbeitsplatzrechnern und Servern sind im Detail im ICT-Konzept geregelt.	Immer	Informationssicherheitsverantwortlicher
Monitoring / Überwachung	Die Verfügbarkeit der Anwendungsdienste sowie die Qualität der gelieferten Monitoringdaten werden laufend überprüft.	Immer	Anwendungs- und Datenverantwortlicher
Netzwerk / Firewall	Alle Netzwerkzugänge werden gesichert. Die vom Kanton vorgegebene Network Security Policy der übergeordneten Netzwerke (LEUnet) wird eingehalten.	Immer	Externer IT-Support Anwendungs- und Datenverantwortlicher
Virenschutz / Internet	Virenschutzprogramme werden auf allen IT-Systemen eingesetzt. Durch entsprechende Massnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben. Ein Webfilter für den Schutz der SuS bei der Arbeit im Internet (Web Protection) ist installiert.	Immer	Externer IT-Support
Datensicherung (Back-up)	Die elektronische Datensicherung wird regelmässig durchgeführt. Die Sicherungsmedien werden an getrennten Orten aufbewahrt und sind physisch geschützt. Es wird gewährleistet, dass verlorene oder fehlerhafte Teile des Informationsbestands über eine ausreichende Dauer wiederhergestellt werden können.	Alle 2 Tage	Externer IT-Support Anwendungs- und Datenverantwortlicher

7.3 Datenspeicherung und -bearbeitung

Name	Beschreibung	Zeitpunkt	Verantwortung
Datenablage	Die Datenablage erfolgt auf dem schuleigenen Server, lokalen Schulgeräten oder in der Cloud (siehe	Immer	Alle Mitarbeitenden und SuS

	spezielle Bestimmungen für besondere Personendaten). Auf die Speicherung auf privaten Geräten ist zu verzichten.		
Besondere Personendaten	An der Primarschule Wettswil dürfen besondere Personendaten nur auf dem Schulserver oder Lehreroffice abgelegt werden, auf keinen Fall in Office365. Die Speicherung besonderer Personendaten auf privaten Geräten oder privaten Clouds ist nicht erlaubt. Papierdokumente mit besonderen Personendaten sind in abgeschlossenen Schränken in den Räumen der Primarschule aufzubewahren.	Immer	Alle Mitarbeitenden
Fotos, Video- und Audioaufnahmen	Werden Fotos, Video- oder Audioaufnahmen mit privaten Geräten vorgenommen, sind diese sofort auf dem Schulserver zu speichern und auf dem privaten Gerät zu löschen	Immer	Alle Mitarbeitenden
Cloud	Als Cloud wird zum einen Office365, zum anderen Lehreroffice unterstützt. Andere Clouds dürfen nicht verwendet werden. Office365 darf nur unter dem zwischen Educa.ch und Microsoft abgeschlossenen Rahmenvertrag betrieben werden. Lehreroffice sichert einen Speicherort in der Schweiz zu.	Immer	Alle Mitarbeitenden und SuS
Datenschutz	Alle Daten werden gemäss den datenschutzrechtlichen Vorgaben bearbeitet.	Nach Bedarf	Informationssicherheitsverantwortlicher
Einsicht	Es existieren Prozesse, um die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Sperrung, Löschung sowie Einsicht sicherzustellen.	Nach Bedarf	Anwendungs- und Datenverantwortlicher

7.4 Datenzugriff

Name	Beschreibung	Zeitpunkt	Verantwortung
Berechtigungsgruppen	Der Zugriff auf die Informationen ist durch Berechtigungsgruppen	Nach Bedarf	Anwendungs- und Datenverantwortlicher

	definiert und geregelt. Die Zugriffsberechtigungen für Mitarbeitende sowie für SuS sind so definiert, dass sie für die Erfüllung der Aufgaben geeignet sind. Ausnahmen werden dokumentiert.		
Passwörter	Die Netzwerke und Systeme sind durch Passwörter zu sichern. Die Zugänge zu allen Daten und Anwendungen sind durch mitarbeiterabhängige Passwörter gesichert. Passwörter werden regelmässig geändert.	Immer	Alle

7.5 Physische Sicherheit

Name	Beschreibung	Zeitpunkt	Verantwortung
Zutritt	Gebäude, Räume und Schränke sowie IT- und Netzwerksysteme werden durch ein ausreichendes Schliesssystem und weitere Massnahmen für die physische Sicherheit angemessen geschützt. Endbenutzergeräte sind zu sperren, wenn der Raum verlassen wird oder sie nicht benutzt werden.	Immer	Schulverwaltung Leitung Liegenschaften
Physische Sicherheit	Massnahmen für die physische Sicherheit sind gewährleistet (Feuer, Wasser, Diebstahl).	Immer	Schulpflege

7.6 Kommunikation

Name	Beschreibung	Zeitpunkt	Verantwortung
Verschlüsselung	Die Datenübertragung von Informationen, die aufgrund ihres Missbrauchspotenzials und der damit zusammenhängenden Risiken einen erhöhten Schutz benötigen, beispielsweise besondere Personendaten, erfolgt in der Regel über die herkömmliche Post. Nur in Ausnahmefällen dürfen solche Informationen per E-Mail verschickt werden. Sie müssen in diesen Fällen immer verschlüsselt werden.	Nach Bedarf	Alle

E-Mail	Besondere Personendaten dürfen nie als E-Mail verschickt werden (Ausnahme siehe Verschlüsselung). Bei der Versendung von Elterninformationen ist zu beachten, dass die E-Mail-Adressen der Eltern zu schützen sind und daher nur als Blind Copy (Bcc) erfasst werden. Anhänge von eingehenden E-Mails sind nur dann zu öffnen, wenn der Absender bekannt ist (Virenschutz).	Immer	Alle
Soziale Netzwerke	Soziale Netzwerke wie Facebook, WhatsApp, Snapchat, Instagram etc. dürfen für die Kommunikation nach aussen wie auch mit den SuS nicht verwendet werden. Die Verwendung ist nur für den Austausch von Belanglosigkeiten erlaubt. Im Zweifel ist E-Mail oder die Chat-Funktion von Office365 vorzuziehen. Bei der privaten Benutzung von sozialen Netzwerken ist die Schweigepflicht zu beachten. Es dürfen keine schulischen Belange oder Begebenheiten erwähnt werden.	Immer	Alle
Allgemeine Kommunikation	Gespräche über schützenswerte Themen (z.B. schwierige Schüler) sind so zu führen, dass keine Unbeteiligten mithören können.	Immer	Alle

8 Qualitätssicherung / Überprüfung des Konzepts

Die Schulpflege unterstützt die Einhaltung und weitere Verbesserung der Informationssicherheit. Das vorliegende Konzept Informationssicherheit und Datenschutz sowie die Massnahmenplanung und -umsetzung des Schutzbedarfs stützt sich auf die gesetzlichen Vorgaben und wird regelmässig im Rahmen des Internen Kontrollsystems (IKS) überprüft. Festgestellte Abweichungen werden innert nützlicher Frist behoben. Die zu ergreifenden Massnahmen orientieren sich am Stand der Technik sowie an nationalen und internationalen Standards.