

# **Konzept Informationssicherheit und Datenschutz**

**der Primarschule Wettswil a.A.**

PSP Nr. 189-10/25

vom 29. September 2025

Inkraftsetzung 1. Januar 2026

## Inhaltsverzeichnis

1	Einleitung	3
2	Allgemeine Bestimmungen .....	3
2.1	Gegenstand und Zweck .....	3
2.2	Geltungsbereich .....	3
2.3	Grundlagen.....	3
3	Informationssicherheitsniveau .....	3
4	Informationssicherheitsziele.....	4
5	Informationssicherheitsorganisation.....	4
5.1	Schulpflege.....	5
5.2	Informationssicherheitsverantwortliche/r .....	5
5.3	Anwendungs- und Datenverantwortliche/r .....	6
5.4	Datenschutzberater/in.....	6
5.5	Operative Leitungen .....	7
6	Schutzbedarf und Zugriffsberechtigungen .....	7
6.1	Schutzbedarfskategorien .....	7
6.2	Zugriffskontrolle (8.8).....	8
6.3	Berechtigungsgruppen.....	8
6.4	Zugriffsmatrizen .....	9
7	Informationssicherheitsmassnahmen.....	10
7.1	Informationssicherheitsorganisation.....	10
7.2	IT-Systeme (8.11).....	13
7.3	Datenspeicherung und -bearbeitung (8.6).....	14
7.4	Datenzugriff .....	16
7.5	Physische Sicherheit (8.10) .....	16
7.6	Kommunikation.....	17
8	Qualitätssicherung / Überprüfung des Konzepts (8.21).....	18

# 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 und des Datenschutzes.

## 2 Allgemeine Bestimmungen

### 2.1 Gegenstand und Zweck

Dieses Konzept regelt die Ziele und die Organisation der Primarschule Wettswil, sowie die allgemeinen Vorgaben in Bezug auf Datenschutz und Informationssicherheit sowie die Prozesse zu deren kontinuierlichen Verbesserung. Es ist angelehnt an die allgemeinen sowie die besonderen Informationssicherheitsrichtlinien des Kantons Zürich.

Ausnahmen zu den in diesem Konzept definierten Vorgaben sind durch die Schulpflege bewilligen zu lassen.

### 2.2 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.

### 2.3 Grundlagen

Die gesetzlichen Grundlagen sind:

- Gesetz über die Information und den Datenschutz (IDG, [LS 170.4](#))
- Verordnung über die Information und den Datenschutz (IDV, [LS 170.41](#))
- Verordnung über die Informationsverwaltung und -sicherheit (IVSV, [LS 170.8](#))

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

## 3 Informationssicherheitsniveau

Die Schulpflege der Primarschule Wettswil hat entschieden, dass ein angemessenes Sicherheitsniveau für einen normalen Schutzbedarf angestrebt werden soll. Diese Einstufung erfolgt aufgrund der Tatsache, dass die Anzahl der betroffenen Personen gering ist, alle wesentlichen Funktionen und Aufgaben durch ICT- und Netzwerksysteme unterstützt werden und ein Ausfall von ICT- und Netzwerksystemen die Aufgabenerfüllung nicht beeinträchtigen sollte. Zudem wurde für diese Entscheidung eine Gefährdungsabschätzung (Schutzbedarfsanalyse) über die Werte der Schutzobjekte sowie des vertretbaren Aufwands an Personal und Finanzmitteln für

Informationssicherheit vorgenommen. Für Datensammlungen mit einem höheren Schutzbedarf werden zusätzliche Sicherheitsmassnahmen getroffen.

## 4 Informationssicherheitsziele

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

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

## 5 Informationssicherheitsorganisation

Die Schulpflege, die/der Informationssicherheitsverantwortliche, die/der Anwendungs- und Datenverantwortliche und die/der Datenschutzberater sowie die operativen Leitungen der einzelnen Bereiche haben zentrale Rollen in der Informationssicherheitsorganisation inne.

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.

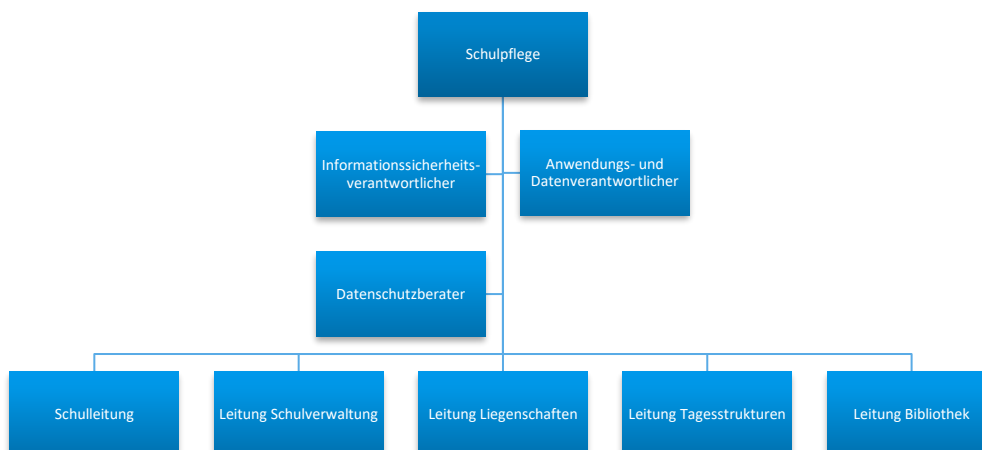


Abb. 1: Organigramm Informationssicherheitsorganisation der Primarschule Wettswil

## 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 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*, *Anwendungs- und Datenverantwortlicher* und *Datenschutzberater* bestimmten Personen zu.

## 5.2 Informationssicherheitsverantwortliche/r

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 die Leitung des Ressorts Informatik und selbst Mitglied der Schulpflege. Die/der Informationssicherheitsverantwortliche ist für die Ausarbeitung und Nachführung des Konzepts Informationssicherheit und Datenschutz verantwortlich, entscheidet über sicherheitsrelevante Fragen und berichtet in dieser Funktion direkt der Schulpflege.

Der/dem Informationssicherheitsverantwortlichen werden ausreichend finanzielle und zeitliche Ressourcen für die Ausübung der Tätigkeit zur Verfügung gestellt. Die Anwendungsverantwortlichen sowie die ICT-Benutzenden unterstützen die/den Informationssicherheitsverantwortlichen. Sie/er wird in alle Projekte involviert, um frühzeitig die sicherheitsrelevanten Aspekte einbringen zu können.

Für sicherheitsrelevante Fragen ist die/der Informationssicherheitsverantwortliche weisungsberechtigt. Sie/er ist die Anlaufstelle für Informationssicherheitsfragen und Hinweise auf Schwachstellen und verfügt über ein angemessenes Wissen sowie entsprechende Fähigkeiten.

*Die Aufgaben der/des Informationssicherheitsverantwortlichen umfassen im Einzelnen:*

- *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*
- *Jährliche Überprüfung sowie Kontrolle der Vollständigkeit der Berechtigungslisten und Zugriffsmatrix im Rahmen des IKS*
- *Beratung der Mitarbeitenden und der Schulpflege in Belangen der Informationssicherheit und des Datenschutzes*
- *Planung und Anordnung von Sensibilisierungs- und Schulungsmassnahmen zum Thema Informationssicherheit*

### **5.3 Anwendungs- und Datenverantwortliche/r**

Für alle Prozesse, Daten, Anwendungen, ICT- 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 der/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 Ausnahmegewilligungen 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*

### **5.4 Datenschutzberater/in**

Der Datenschutz und die Informationssicherheit sind für alle Bereiche, in denen personenbezogene Daten verarbeitet werden, von grundlegender Bedeutung. Zur Umsetzung des Datenschutzes wird eine Person bestimmt, die für den Datenschutz verantwortlich ist. Die Datenschutzberaterin/der Datenschutzberater arbeitet in dieser Rolle eng mit den Informationssicherheitsverantwortlichen zusammen und ist interne Ansprechperson bei Datenschutzfragen.

*Aufgaben der Datenschutzberaterin/des Datenschutzberaters:*

- *Ansprechperson für Mitarbeitende sowie für die Schulpflege in Belangen des Datenschutzes*
- *Bindeglied zur kantonalen Datenschutzbeauftragten (DSB) bei Fragen zum Datenschutz*
- *Zuständige Person für die Einhaltung der gesetzlichen Meldepflicht bei Datenschutzvorfällen*
- *Ansprechperson für Betroffene in Sachen Datenschutz (Auskunfts- und Löschbegehren)*
- *Bericht an die Schulpflege über den Stand des Datenschutzes*
- *Planen, koordinieren und umsetzen von Sensibilisierungs- und Schulungsmassnahmen zum Thema Datenschutz*

## **5.5 Operative Leitungen**

Die operativen Leitungen 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 (8.8)

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 ICT-Systeme (Server, Endbenutzergeräte, Netzwerke) und Anwendungen (Office365, Schulportal, E-Mail, Scholaris, Lehreroffice etc.). Jeder Anwendende wird mindestens durch eine Identifikation und ein Passwort gegenüber dem System identifiziert und authentifiziert. Bezüglich Zugriff auf Informationen wird unterschieden zwischen: Kein Zugriff, Lesen, Bearbeiten und Löschen.

Sämtliche Zugriffsberechtigungen werden mindestens jährlich geprüft. Bei Austritt von Mitarbeitenden werden deren Zugriffsrechte umgehend entfernt bzw. deaktiviert. Verwaltungseigene Hardware wird spätestens bei Austritt zurückgenommen.

Die Art und Stärke der Authentifizierung werden durch die Klassifizierung der Information und die Exponiertheit der Anwendung bestimmt, auf die der Zugriff erfolgen soll. Zugriffsrechte für administrative Zugriffe werden restriktiv und kontrolliert vergeben. Es ist jederzeit nachvollziehbar, wer welche Zugriffsrechte besitzt.

ICT-Systeme, Netzwerkkomponenten und die Abtrennung des internen Netzwerks von Fremdnetzen (Firewall) werden von einem externen Auftragnehmer 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 Auftragnehmer 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 Schulleitungen
Leitung Tagesstrukturen	Leitung Tagesstrukturen
Leitung Bibliothek	Leitung Bibliothek
Leitung Liegenschaften	Leitung 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 vier 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 ICT-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 3) 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 der Fall auftreten, dass die Zugriffsberechtigung nicht allen Personen einer Berechtigungsgruppe gewährt wird, sondern nur einzelnen Personen einer Gruppe.

Die/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. Die/der Informations-sicherheitsverantwortliche 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 Auftragnehmer erbracht, ist die Schule dafür verantwortlich, dass die erforderlichen Sicherheitsmassnahmen umgesetzt werden.

### 7.1 Informationssicherheitsorganisation

Name	Beschreibung	Zeitpunkt	Verantwortung
<b>Organisation</b>	Das Organigramm Informations-sicherheitsorganisation (Seite 5) regelt alle Funktionen sowie deren Stellvertretung. Durch ausreichende Dokumentation und Instruktion soll sichergestellt werden, dass die Stellvertreter ihre Aufgabe erfüllen können.	Immer	Informationssicherheitsverantwortlicher Anwendungs- und Datenverantwortlicher Datenschutzberater
<b>Outsourcing</b> (8.16)	Bei der Auslagerung von Datenbearbeitungen werden der Datenschutz und die Informationssicherheit gewährleistet, indem schriftliche Verträge abgeschlossen und entsprechende Kontrollmassnahmen vereinbart werden.  Benötigt eine externe Stelle oder der interne IT-Betrieb den Einsatz von Fernwartungszugängen, werden diese nur nach entsprechendem Antrag freigegeben und auf die nötigsten Systeme und Zeiten begrenzt.  Vor der Gewährung von Fernwartungszugängen erfolgt eine angemessene Sicherheitsüberprüfung, eine Geheimhaltungsverpflichtung wird unterzeichnet und entsprechende vertragliche Regelungen werden abgeschlossen. Dasselbe gilt für den Einsatz von Fremdpersonal.	Nach Bedarf	Informationssicherheitsverantwortlicher
<b>Eintritt und Austritt von Mitarbeitenden</b>	Der beim Eintritt oder Austritt von Mitarbeitenden durchlau-	Immer	Operative Leiter

	<p>fene Prozess beinhaltet die Information über das Konzept Informationssicherheit und Datenschutz. Neueintretende unterzeichnen eine <a href="#">Nutzungsvereinbarung</a>. Bei Austritt bestätigt der Austretende mit seiner Unterschrift, dass alle schulischen Daten auf persönlichen Geräten (inkl. Backups) gelöscht wurden.</p>		
<b>Sensibilisierung</b>	<p>Mindestens einmal jährlich informieren die operativen Leitungen die Mitarbeitenden über die Informationssicherheit, den Datenschutz, aktuelle Gefahren und zu treffende Massnahmen (Audit). Zusätzlich werden auch Sensibilisierungsprogramme durchgeführt, deren Ziele sind:</p> <ul style="list-style-type: none"> <li>• Bewusstsein für Informationssicherheit und Datenschutz schaffen und Grundwissen vermitteln</li> <li>• Spezifische Kenntnisse für die jeweiligen Fachaufgaben bezüglich Informationssicherheit und/oder Datenschutz vermitteln</li> <li>• Vermitteln, wie bei sicherheitskritischen Situationen zu reagieren ist und dauerhafte Verhaltensänderung erzielen</li> </ul>	Jährlich	Alle
<b>Weisungen</b>	<p>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.</p>	Immer	Alle

	Die Lehrpersonen instruieren die SuS betreffend Informationssicherheit.		
<b>Informationssicherheitsvorfälle (8.17)</b>	<p>Bei Informationssicherheitsvorfällen erfolgt durch die bzw. den Informationssicherheitsverantwortlichen eine Klassifizierung und wenn nötig sofortige Reportierung an die Schulpflege. Entsprechende interne Prozesse und Verfahren für Meldung, Aufnahme von Beweismitteln zwecks rechtlicher und/oder disziplinarischer Massnahmen sowie eine angemessene Eskalation sind geregelt (siehe dazu auch Notfallkonzept).</p> <p>Bei meldepflichtigen Informationssicherheitsvorfällen (Gefährdung von Grundrechten durch die unbefugte Bearbeitung oder den Verlust von Personendaten) erstattet die Schulpflege unverzüglich nach Bekanntwerden des Vorfalls bei der DSB Meldung (§ 12a IDG). Bei Zweifeln über das Vorliegen einer Meldepflicht erfolgt eine unverzügliche Kontaktaufnahme mit der DSB. Im Notfallkonzept sind mögliche Informationssicherheitsvorfälle und Massnahmen zu definiert.</p> <p>Alle Informationssicherheitsvorfälle werden nachvollziehbar dokumentiert. Die Informationen sind als vertraulich zu betrachten.</p>	Immer	Schulpflege

## 7.2 IT-Systeme (8.11)

Aus der Definition der Informationssicherheitsziele ergeben sich folgende Massnahmen:

Name	Beschreibung	Zeitpunkt	Verantwortung
<b>ICT-Systeme</b>	Die ICT-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
<b>Aktualisierungen/ Updates</b>	Alle ICT-Systeme und Anwendungen werden regelmässig aktualisiert und mit den aktuellsten Sicherheitsupdates versorgt.	wöchentlich	Externer IT-Support
<b>Archivierung / Löschung (8.20)</b>	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
<b>Mobile Geräte / Software (8.1)</b>	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. Für Daten mit erhöhtem Risiko auf Missbrauch werden die entsprechenden technischen und organisatorischen Massnahmen ergriffen.	Immer	Informationssicherheitsverantwortlicher
<b>Wechselmedien (8.7)</b>	Der Einsatz von Wechselmedien erfolgt kontrolliert, darauf enthaltene dienstliche Daten werden vor Zugriff von Dritten und Verlust geschützt.		
<b>Monitoring / Überwachung</b>	Die Verfügbarkeit und Qualität der Anwendungsdienste werden laufend überprüft.	Immer	Anwendungs- und Datenverantwortlicher

<b>Netzwerk / Firewall</b> (8.14)	Alle Netzwerkzugänge werden gesichert. Schutzmechanismen werden so konfiguriert und administriert, dass sie einen wirkungsvollen Schutz gewährleisten und Manipulationen verhindern. Die vom Kanton vorgegebene Network Security Policy der übergeordneten Netzwerke (LEUnet) wird eingehalten.	Immer	Externer IT-Support  Anwendungs- und Datenverantwortlicher
<b>Virenschutz / Internet</b>	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
<b>Datensicherung (Back-up)</b> (8.12)	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
<b>Inventar</b> (8.5)	Als Inventar gilt die Doku der Firma Letec IT Solutions AG, welche sämtliche Geräte auflistet.	Immer	Externer IT-Support / Verantwortlicher IT Support

### 7.3 Datenspeicherung und -bearbeitung (8.6)

Name	Beschreibung	Zeitpunkt	Verantwortung
<b>Datenablage</b>	Die Datenablage erfolgt auf dem schuleigenen Server, lokalen Schulgeräten oder in der Cloud (siehe spezielle Bestimmungen für besondere Personendaten). Auf die Speicherung auf privaten Geräten ist zu verzichten.	Immer	Alle Mitarbeitenden und SuS

<b>Besondere Personendaten</b>	An der Primarschule Wettswil dürfen besondere Personendaten nur auf dem Schulserver oder auf CMI Sclaris/Lehreroffice/Protokolle/Sitzungen/Dossier abgelegt werden. Diese Daten dürfen nicht in den üblichen Office365-Anwendungen (Teams, Outlook) verwendet werden. 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
<b>Fotos, Video- und Audioaufnahmen</b>	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
<b>Cloud</b>	Als Cloud wird zum einen Office365, zum anderen Lehreroffice/Sclaris unterstützt. Andere Clouds dürfen nicht verwendet werden. Office365 darf nur unter dem zwischen Educa.ch und Microsoft abgeschlossenen Rahmenvertrag betrieben werden. CMI sichert für Lehreroffice und Sclaris einen Speicherort in der Schweiz zu.	Immer	Alle Mitarbeitenden und SuS
<b>Datenschutz</b>	Alle Daten werden gemäss den datenschutzrechtlichen Vorgaben bearbeitet.	Nach Bedarf	Informationssicherheitsverantwortlicher
<b>Einsicht</b>	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
<b>Berechtigungsgruppen</b> (8.8)	Der Zugriff auf die Informationen ist durch Berechtigungsgruppen definiert und geregelt. Die Zugriffsberechtigungen der Behördenmitglieder, der Mitarbeitenden sowie der SuS auf Systeme und Netzwerke sind so definiert, dass sie für die Erfüllung der Aufgaben geeignet sind. Ausnahmen werden dokumentiert.	Nach Bedarf	Anwendungs- und Datenverantwortlicher
<b>Passwörter</b> (8.9)	Die Netzwerke und Systeme sind durch Passwörter zu sichern. Die Zugänge zu allen Daten und Anwendungen sind durch mitarbeiterabhängige Passwörter gesichert. Es wird eine ausreichende Qualität der Passwörter sichergestellt.  Wenn erforderlich wird mit Mehrfaktorauthentifizierung gearbeitet.	Immer	Alle

## 7.5 Physische Sicherheit (8.10)

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

## 7.6 Kommunikation

Name	Beschreibung	Zeitpunkt	Verantwortung
<b>Verschlüsselung</b> (8.4)	Die Datenübertragung von Informationen, die aufgrund ihres Missbrauchspotenzials und der damit zusammenhängenden Risiken einen erhöhten Schutz benötigen, beispielsweise besondere Personendaten, erfolgt verschlüsselt über öffentliche Netzwerke oder über die herkömmliche Post.	Nach Bedarf	Alle
<b>E-Mail</b>	<p>Besondere Personendaten dürfen nur verschlüsselt und über sichere Mail-Dienste verschickt werden.</p> <p>Elterninformationen werden meistens über Klapp verschickt. 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.</p> <p>Anhänge von eingehenden E-Mails sind nur dann zu öffnen, wenn der Absender bekannt ist (Virenschutz).</p>	Immer	Alle
<b>Soziale Netzwerke</b>	<p>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.</p> <p>Bei der privaten Benutzung von sozialen Netzwerken ist die Schweigepflicht zu beachten. Es dürfen keine schulischen Belange oder Begebenheiten erwähnt werden.</p>	Immer	Alle

	Die digitale Kommunikation Lehrpersonen + Eltern erfolgt ausschliesslich über Klapp.		
<b>Allgemeine Kommunikation</b>	Gespräche über schützenswerte Themen (z.B. schwierige Schüler) sind so zu führen, dass keine Unbeteiligten mithören können.	Immer	Alle

## 8 Qualitätssicherung / Überprüfung des Konzepts (8.21)

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.