

## Leitlinie zur Informationssicherheit

(genehmigt an der Schulpflegesitzung vom 4. März 2025)

### 1 EINLEITUNG

Die Primarschule Boppelsen ist zur 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 diese Leitlinie zur Informationssicherheit. Sie trägt zum Datenschutz und zur Informationssicherheit bei, indem sie das von der Primarschule Boppelsen angestrebte Informationssicherheitsniveau, die Informationssicherheitsziele sowie die geeigneten Massnahmen definiert. Weiter beinhaltet die Leitlinie eine Beschreibung der Informationssicherheitsorganisation.

### 2 GELTUNGSBEREICH

Die Leitlinie zur Informationssicherheit und die damit zusammenhängenden Dokumente gelten für alle Mitarbeitenden und die Behördenmitglieder der Primarschule Boppelsen. Vertragspartner, die Daten bearbeiten, werden zur Einhaltung der im Folgenden aufgeführten Anforderungen verpflichtet.

### 3 INFORMATIONSSICHERHEITSNIVEAU

Die Schulpflege der Primarschule Boppelsen hat entschieden, dass ein angemessenes Sicherheitsniveau für einen normalen Schutzbedarf angestrebt werden soll. Grundlage für diese Entscheidung war eine Gefährdungsabschätzung über die Werte der Schutzobjekte sowie des vertretbaren Aufwands an Personal und Finanzmitteln für Informationssicherheit. Für Datensammlungen mit einem höheren Schutzbedarf werden zusätzliche Sicherheitsmassnahmen getroffen.

### 4 INFORMATIONSSICHERHEITSZIELE

Aus der Einstufung ergeben sich die folgenden Informationssicherheitsziele (§ 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, IKT-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 Verwaltungsbetrieb haben.
<b>Vertraulichkeit</b>	Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen.
<b>Zurechenbarkeit</b>	Informationsbearbeitungen müssen einer Person zugerechnet werden können.

## 5 INFORMATIONSSICHERHEITSMASSNAHMEN

Die Auswahl der technischen und organisatorischen Massnahmen erfolgt anhand der Anforderungen der ISO/IEC 27001 und den Standards des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI):

<b>Aktualisierungen (Updates)</b>	Alle IKT-Systeme (Server, Clients und Netzwerkkomponenten) werden regelmässig aktualisiert und mit den aktuellsten Sicherheitsupdates versorgt.
<b>Archivierung / Löschung</b>	Alle Daten werden gemäss den regulatorischen Vorgaben archiviert. Falls eine Aufbewahrung nicht mehr erforderlich ist, werden diese sicher gelöscht.
<b>Berechtigungskonzept</b>	Der Zugriff auf die Informationen ist durch ein Berechtigungskonzept geregelt. Die Zugriffsberechtigungen der Behördenmitglieder, der Mitarbeitenden sowie der Lernenden auf Systeme und Netzwerke sind für die Erfüllung der Aufgaben erforderlich und geeignet.
<b>Datenschutz</b>	Alle Daten werden gemäss den datenschutzrechtlichen Vorgaben bearbeitet. Es existieren Prozesse, um die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Sperrung, Löschung sowie Einsicht sicherzustellen.
<b>Datensicherung (Backup)</b>	Die 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.
<b>IKT-Systeme</b>	Die IKT-Systeme werden nach der Beschaffung sicher installiert (gemäss anerkannten Sicherheitsstandards) und betrieben, mit einem Änderungsmanagement verwaltet und in einem geregelten Prozess ausser Betrieb genommen.
<b>Mobile Geräte / Software</b>	Der Einsatz von Arbeitsplatzrechnern und mobilen Geräten inklusive der Verwendung von privaten Geräten (Bring Your Own Device) sowie der Installation von Software auf Arbeitsplatzrechnern und Servern sind im Detail geregelt. Für Daten mit erhöhtem Risiko auf Missbrauch werden die entsprechenden technischen und organisatorischen Massnahmen ergriffen.
<b>Überwachung (Monitoring)</b>	Die Verfügbarkeit und Qualität der Anwendungsdienste werden laufend überprüft.
<b>Netzwerk / Firewall</b>	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.
<b>Organisation</b>	Die relevanten Funktionen der Organisation sind festgelegt und in einem Organigramm dokumentiert. Für alle Funktionen ist die Stellvertretung geregelt. Durch ausreichende Dokumentation und Instruktion wird sichergestellt, dass die Stellvertretenden ihre Aufgabe erfüllen können.

<b>Outsourcing</b>	Bei der Auslagerung von Datenbearbeitungen werden der Datenschutz und die Informationssicherheit gewährleistet, indem schriftliche Verträge abgeschlossen und entsprechende Kontrollmassnahmen vereinbart werden.
<b>Passwörter</b>	Die Zugänge zu allen Systemen, Daten und Anwendungen sind durch mitarbeiterabhängige Passwörter gesichert. Es wird eine ausreichende Qualität der Passwörter sichergestellt.
<b>Sensibilisierung / Schulung</b>	Die Mitarbeiterinnen und Mitarbeiter werden regelmässig über aktuelle Gefahren und zu treffende Massnahmen informiert.
<b>Verschlüsselung</b>	Die Datenübertragung von Informationen, die aufgrund ihres Missbrauchspotenzials und der damit zusammenhängenden Risiken einen erhöhten Schutz benötigen, beispielsweise besondere Personendaten, erfolgt verschlüsselt über öffentliche Netze.
<b>Virenschutz / Internet</b>	Virenschutzprogramme werden auf allen IKT-Systemen eingesetzt. Durch entsprechende Massnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.
<b>Weisungen</b>	Die Mitarbeiterinnen und Mitarbeiter 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.
<b>Zutritt</b>	Gebäude und Räume sowie IKT- und Netzwerksysteme werden durch ein ausreichendes Schliesssystem und weitere Massnahmen für die physische Sicherheit angemessen geschützt.
<b>Physische Sicherheit</b>	Brandschutzmassnahmen, Zutrittskontrolle usw.

## 6 INFORMATIONSSICHERHEITSORGANISATION

Die Schulpflege, die Informationssicherheitsverantwortliche/der Informationssicherheitsverantwortliche (ISV) und die für die einzelnen Bereiche zuständigen Daten- und Anwendungsverantwortlichen haben die zentralen Rollen in der Informationssicherheitsorganisation inne.

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

### SCHULPFLEGE

Die Schulpflege trägt die Gesamtverantwortung für die Informationssicherheit in der Primarschule Boppelsen. Sie legt die Leitlinie zur Informationssicherheit fest und genehmigt die für die Informationssicherheit erforderlichen Massnahmen und Mittel. Sie weist die Rolle / Funktion Informationssicherheitsverantwortliche / Informationssicherheitsverantwortlicher einer verantwortlichen Person zu.

### **Informationssicherheitsverantwortliche/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. Sie ist für die Ausarbeitung und Nachführung eines Sicherheitskonzepts verantwortlich und berichtet in dieser Funktion direkt der ihr oder ihm vorgesetzten Stelle.

Der oder dem ISV werden ausreichende finanzielle und zeitliche Ressourcen für die Ausübung ihrer/seiner Tätigkeit zur Verfügung gestellt. Die IKT- und Anwendungsverantwortlichen sowie die IKT-Benutzerinnen und -Benutzer unterstützen sie/ihn in ihrer/seiner Tätigkeit. Sie/er wird in alle Projekte involviert, um frühzeitig die sicherheitsrelevanten Aspekte einbringen zu können.

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

### **Anwendungs- und Datenverantwortliche**

Für alle Prozesse, Daten, Anwendungen, IKT- und Netzwerksysteme wird eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf (Klassifizierung) bestimmt und die Zugriffsberechtigungen vergibt.

### **Datenschutzberaterin/Datenschutzberater**

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.

## **7 KONTINUIERLICHE VERBESSERUNG DER INFORMATIONSSICHERHEIT**

Die Schulpflege unterstützt die Einhaltung und weitere Verbesserung des Informationssicherheitsniveaus. Sie gibt mit der periodischen Überarbeitung dieser Leitlinie zur Informationssicherheit die notwendigen Leitplanken für eine sichere und gesetzeskonforme Informationsverarbeitung. Die Leitlinie wird periodisch überprüft.

Das Informationssicherheitskonzept und deren Umsetzung wird regelmässig sowie zusätzlich bei Projekten mit grossen Auswirkungen auf den Datenschutz und Informationssicherheit auf die Aktualität und die Wirksamkeit geprüft. Festgestellte Abweichungen werden innert nützlicher Frist behoben.

Die zu ergreifenden Massnahmen orientieren sich am Stand der Technik sowie an nationalen und internationalen Standards.

Primarschulpflege Boppelsen

Sabine Cantaro	Brigitte Frischknecht
Präsidium	Schulverwaltung