

Informationssicherheit für Volksschulen

Workshop Teil 2

Zürich, 10. November 2021



Building Competence. Crossing Borders.

Herzlich Willkommen

Liebe Kurs-Teilnehmer des VSA

Herzlich Willkommen zur heutigen zweiten Teil der Veranstaltung zur Informationssicherheit für Volksschulen!

Schön, dass Sie hier sind, wir freuen uns auf den Kurs mit Ihnen!

Ihr ZHAW-Team

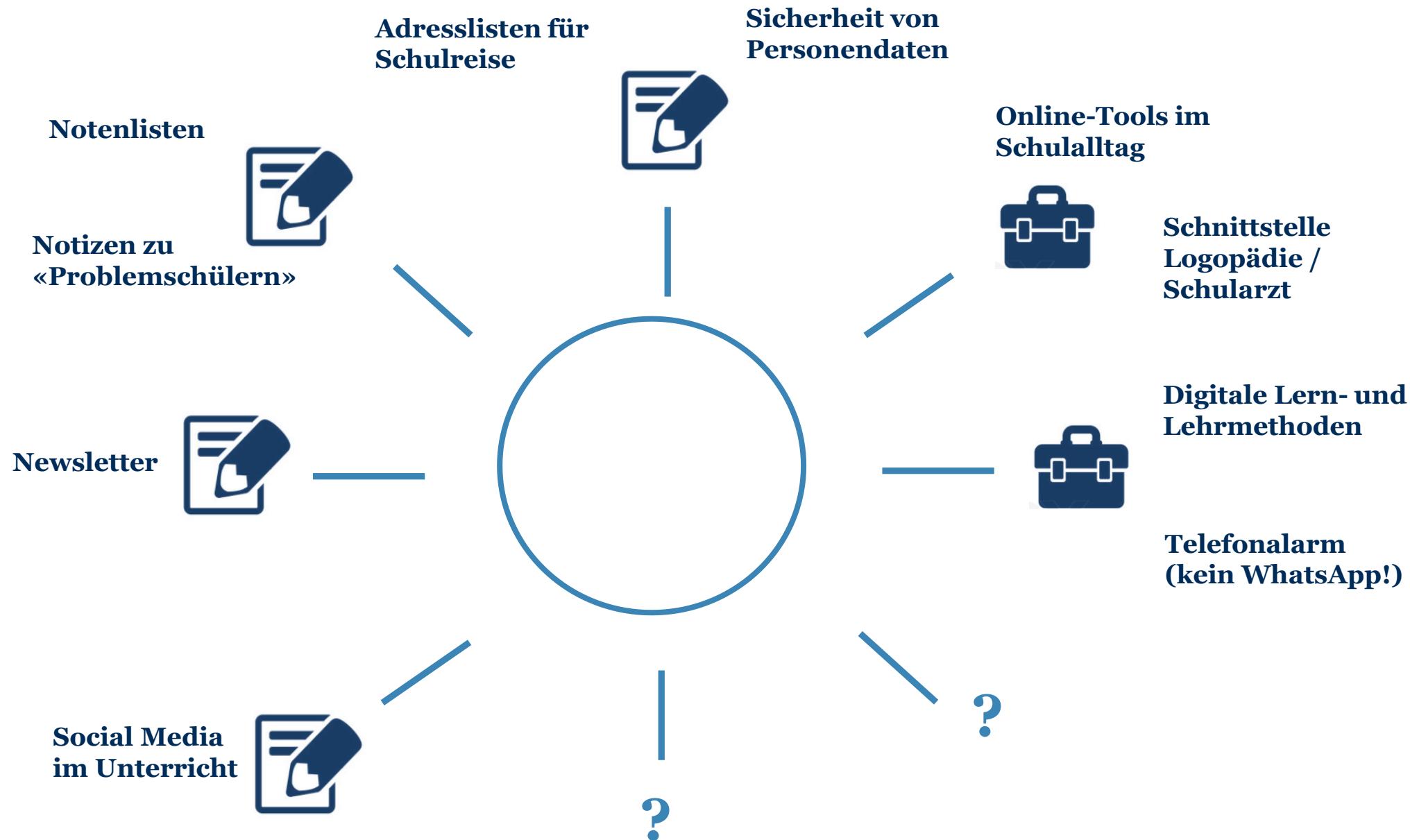
RA Dr. Michael Widmer & RA Marcel Griesinger

Überblick zum heutigen Workshop

Agenda

| | |
|-------------------|-------------------------------------------------------------------|
| 8.00 – 8.20 Uhr | Einführung (René Moser) |
| 8.20 – 8.40 Uhr | Repetition Tag 1 und Überblick über alle Dokumente(Dokumente 1-8) |
| 8.40 – 9.00 Uhr | Besprechung der einzelnen Dokumente, Teil 1 (Dokument 1) |
| 9.00 – 9.10 Uhr | Pause |
| 9.10 – 10.10 Uhr | Besprechung der einzelnen Dokumente Teil 2 (Dokumente 2, 8, 7) |
| 10.10 – 10.30 Uhr | Kaffeepause |
| 10.30 – 11.10 Uhr | Besprechung der einzelnen Dokumente Teil 3 (Dokumente 3, 4, 5, 6) |
| 11.10 – 11.15 Uhr | Pause |
| 11.15 – 11.45 Uhr | Abschliessende Besprechung (René Moser) |
| 11.45 – 12.00 Uhr | Q&A |

Repetition Workshop-Tag 1:



Repetition Workshop-Tag 1:



170.4

Gesetz über die Information und den Datenschutz (IDG)

(vom 12. Februar 2007)^{1,2}

Der Kantonsrat,

nach Einsichtnahme in die Anträge des Regierungsrates vom 9. November 2005³ und der Kommission für Staat und Gemeinden vom 15. September 2006,

beschliesst:

I. Allgemeine Bestimmungen

§ 1. ¹ Dieses Gesetz regelt den Umgang der öffentlichen Organe mit Informationen. Gegenstand und Zweck

² Es bezweckt,

- a. das Handeln der öffentlichen Organe transparent zu gestalten und damit die freie Meinungsbildung und die Wahrnehmung der demokratischen Rechte zu fördern sowie die Kontrolle des staatlichen Handelns zu erleichtern,
- b. die Grundrechte von Personen zu schützen, über welche die öffentlichen Organe Daten bearbeiten.

§ 2.²⁸ Dieses Gesetz gilt für die öffentlichen Organe.

Geltungsbereich

² a.²⁷ ¹ Dieses Gesetz gilt nicht für das Verhältnis zwischen dem Kantonsrat und seinen ständigen Kommissionen sowie den Behörden und Anstalten, die seiner Oberaufsicht unterstehen.

Ausnahmen

a. Kantonsrat

² Soweit der Kantonsrat diesem Gesetz untersteht, stehen der oder dem Beauftragten für den Datenschutz die Befugnisse gemäss § 10 Abs. 2, § 12 a Abs. 1 und 2, § 34 lit. c, d und f sowie §§ 35–36 a nicht zu.

§ 2 b.²⁷ ¹ Bei Gerichtsverfahren sowie Verfahren von Strafverfolgungsbehörden gemäss § 86 Abs. 1 lit. b und c des Gesetzes über die Gerichts- und Behördenorganisation im Zivil- und Strafprozess vom 10. Mai 2010²² richten sich die Rechte der betroffenen Personen und die Einsichtsrechte Dritter nach den spezialgesetzlichen Bestimmungen.

b. Gerichte und Strafverfolgungsbehörden

² Für die Bearbeitung von Personendaten gilt dieses Gesetz, soweit Spezialgesetze keine Regelungen enthalten.

Gesetz über die Information und den Datenschutz (IDG) des Kantons Zürich, LS 170.4

Anwendbar auf kantonale öffentliche Organe, inkl.
Gemeinden.

Direktlink: https://www.zh.ch/de/politik-staat/gesetze-beschluesse/gesetzessammlung/zhlex-ls/erlass-170_4-2007_02_12-2008_10_01-109.html

Weitere rechtliche Grundlagen:

- Verordnung über die Information und den Datenschutz (IDV), LS 170.41
- Verordnung über die Informationsverwaltung und –sicherheit (IVSV), LS 170.8

Repetition Workshop-Tag 1:

Zentrale Vorschrift im Zusammenspiel von Datenschutz und Datensicherheit ist

§ 7 IDG-ZH (Gesetz über die Information und den Datenschutz):

§ 7 IDG (Informationssicherheit)

1 Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen.

2 Die Massnahmen richten sich nach den folgenden Schutzz Zielen:

- a. Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen,
- b. Informationen müssen richtig und vollständig sein,
- c. Informationen müssen bei Bedarf vorhanden sein,
- d. Informationsbearbeitungen müssen einer Person zugerechnet werden können,
- e. Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.

3 Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik.

Repetition Workshop-Tag 1:

Wesentliche Umsetzungserfordernisse und Umsetzungsmassnahmen werden im **Leitfaden der Datenschutzbeauftragten des Kantons Zürich zur Informationssicherheit** in Volksschulen dargestellt.

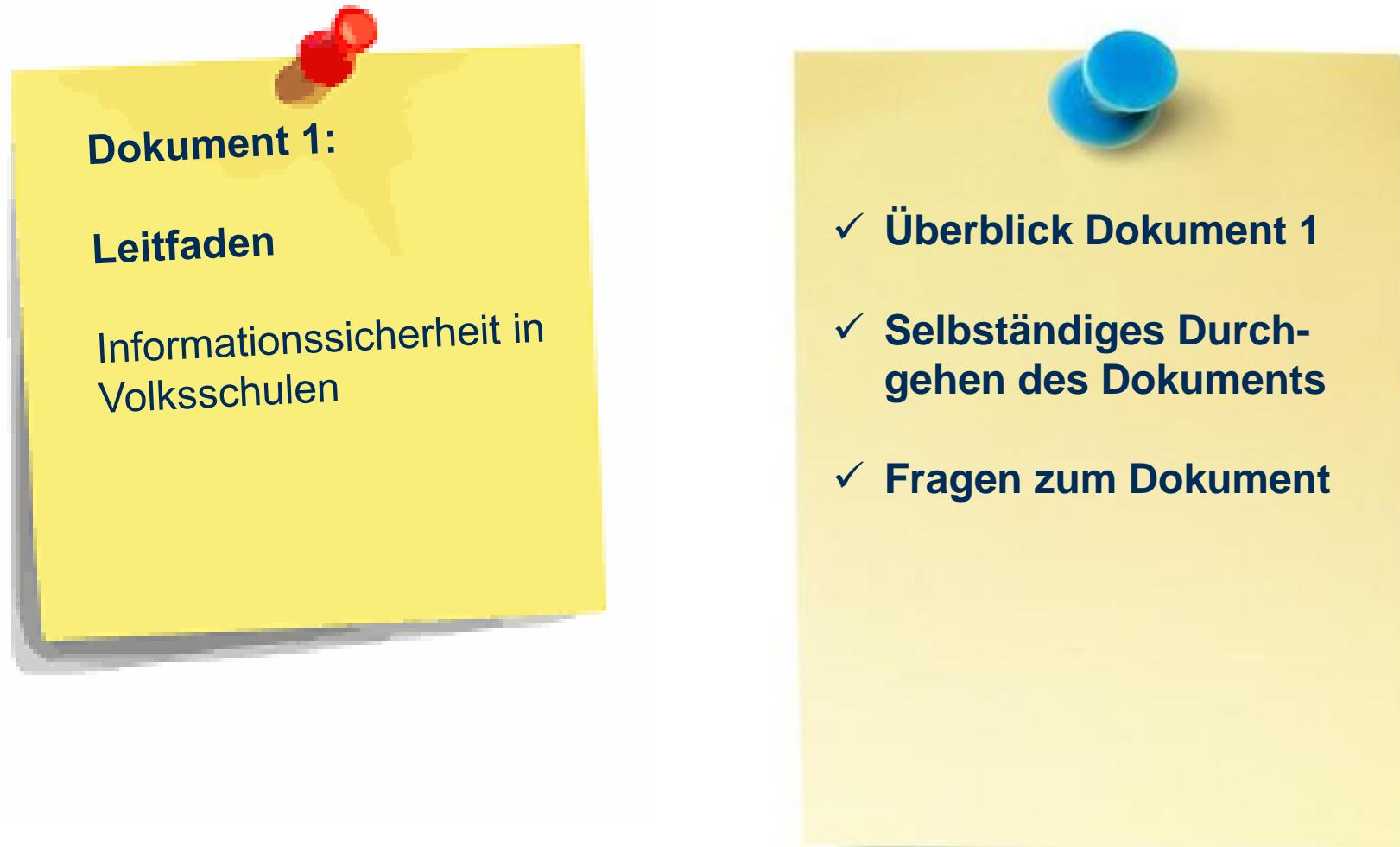
Zur konkreten Umsetzung der zentralen Anforderungen an die Datensicherheit werden unterschiedliche **Vorlagen-Dokumente** von der Datenschutzbeauftragten bereit gehalten.

Wir möchten mit dabei insbesondere die Bereiche **«Sicherheitsstrategie»**, **«Organisationsstruktur»**, **«Schutzbedarfsermittlung»** und **«Sicherheitsmassnahmen»** vertiefen.

Dokumente 1 – 8

Dokumente 1 – 8: Let's go!

Dokument 1 – Leitfaden: Informationssicherheit in Volksschulen

- 
- Dokument 1:**
Leitfaden
**Informationssicherheit in
Volksschulen**
- ✓ **Überblick Dokument 1**
 - ✓ **Selbständiges Durch-
gehen des Dokuments**
 - ✓ **Fragen zum Dokument**

Dokument 1 – Leitfaden: Informationssicherheit in Volksschulen

Was ist zu tun:

1. Überblick betreffend Inhalte Leitfaden und Dokumente verschaffen
2. Schritte 1 – 5 zur Informationssicherheit umsetzen
3. Massnahmen zur Sicherstellung des Schutzniveaus einführen

Zu Ziff. 2: Übersicht Dokumente (vgl. S. 3)

- ✓ Dokument 1 – Leitfaden: Informationssicherheit in Volksschulen
- ✓ Dokument 2 – Vorlage: Leitlinie zur Informationssicherheit in Volksschulen
- ✓ Dokument 3 – Vorlage: Weisung zur Informationssicherheit in Volksschulen
- ✓ Dokument 4 – Anleitung: Sensibilisierung der Mitarbeitenden für Informationssicherheit
- ✓ Dokument 5 – Vorlage: Rollen- und Berechtigungskonzept in Volksschulen
- ✓ Dokument 6 – Erklärung über die Nutzung von Internet/ E-Mail/Informationssicherheit in Volksschulen
- ✓ Dokument 7 - Minimummassnahmenkatalog
- ✓ Dokument 8 - Schutzbedarf feststellung

Dokument 1 – Leitfaden: Informationssicherheit in Volksschulen

Zu Ziff. 3: Umsetzung Anforderungen an die Informationssicherheit (vgl. S. 3 ff.)

1. Sicherheitsstrategie festlegen
2. Organisationsstruktur für Informationssicherheit aufbauen
3. Schutzbedarf festlegen
4. Sicherheitsmassnahmen planen
5. Fehlende Sicherheitsmassnahmen umsetzen

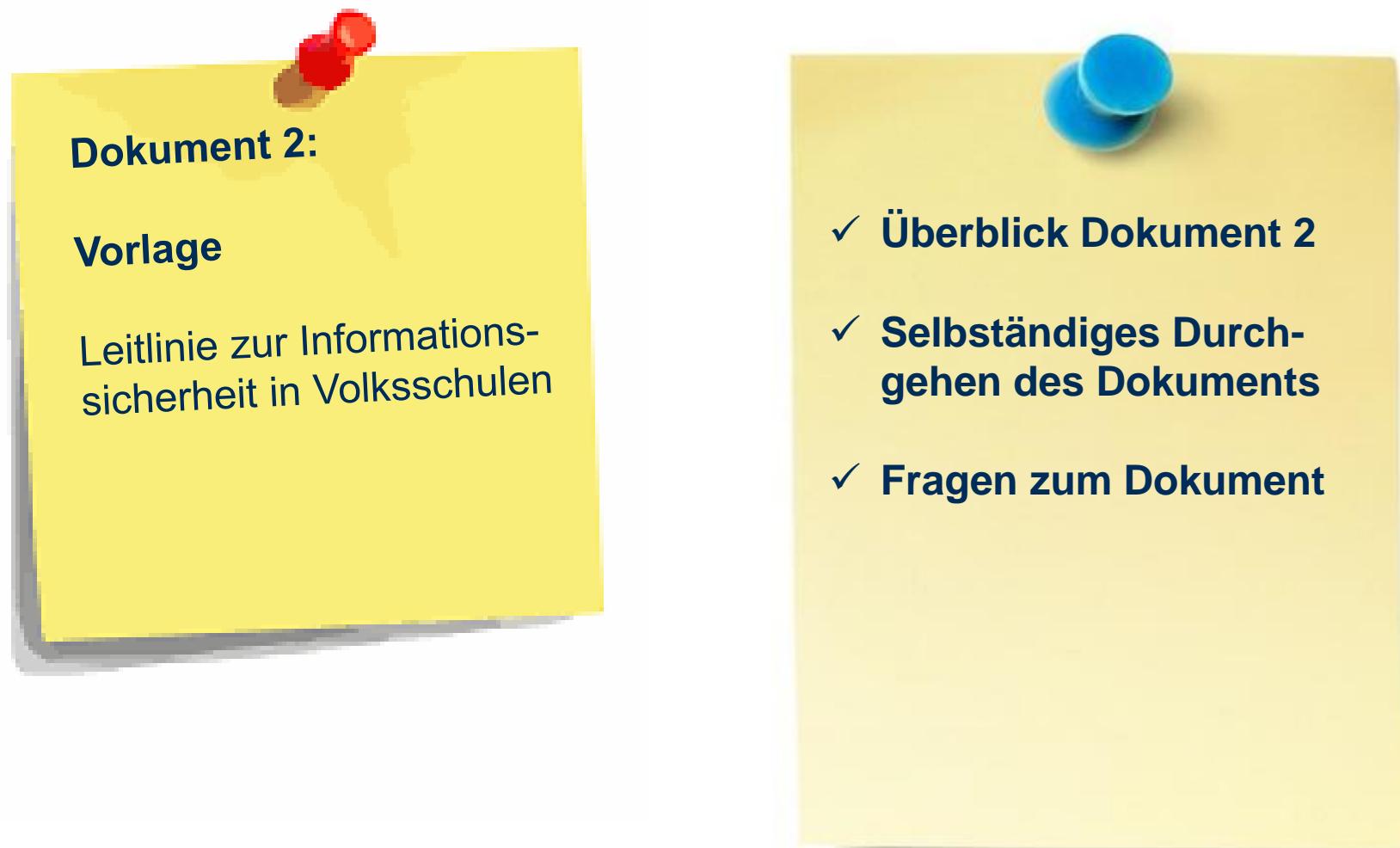
Zu Ziff. 4: Kontinuierliches Erhalten des Sicherheitsniveaus (vgl. S. 8)

1. Regelmässige Überprüfung, dass die erforderlichen Massnahmen umgesetzt werden
2. Regelmässige Überprüfung der Massnahmen an sich

Zu Ziff. 5: Links (vgl. S. 8)

weiterführende Hinweise

Dokument 2 – Vorlage: Leitlinie zur Informationssicherheit in Volksschulen

- 
- Dokument 2:**
Vorlage
Leitlinie zur Informations-
sicherheit in Volksschulen
- ✓ Überblick Dokument 2
 - ✓ Selbständiges Durch-
gehen des Dokuments
 - ✓ Fragen zum Dokument

Dokument 2 – Vorlage: Leitlinie zur Informationssicherheit in Volksschulen

Was ist zu tun:

1. Überblick betreffend Inhalte der Vorlage zur Leitlinie verschaffen
2. Schritte 1 – 6 prüfen und für die konkrete Anwendung hin verwenden und erforderlichenfalls anpassen
3. Beschlussfassung durch die Schulpflege betreffend Leitlinie herbeiführen

Zu Ziff. 1-3: Einleitung/Geltungsbereich/Sicherheitsniveau (vgl. S. 2)

Text prüfen und auf konkrete Einrichtung hin ergänzen

Zu Ziff. 4: Informationssicherheitsziele (vgl. S. 2)

Ziele prüfen und Text erforderlichenfalls ggf. ergänzen

Dokument 2 – Vorlage: Leitlinie zur Informationssicherheit in Volksschulen

Zu Ziff. 5: Informationssicherheitsmassnahmen (vgl. S. 3 f.)

1. Sicherheitsmassnahmen prüfen
2. Sicherheitsmassnahmen auf konkrete Einrichtung hin ergänzen/anpassen

Zu Ziff. 6: Informationssicherheitsorganisation (vgl. S. 4 ff.)

1. Massnahmen zur Informationssicherheitsverantwortung/Rollenzuweisung
 - Informationssicherheitsverantwortliche/r
 - Anwendungs- und Datenverantwortlicher
 - Datenschutzberater/in
2. Massnahmen zur kontinuierlichen Verbesserung der Informationssicherheit

Dokument 2 – Vorlage: Leitlinie zur Informationssicherheit in Volksschulen

Fragen

Über welches Wissen muss die Schulpflege verfügen, damit sie die Verantwortung für die Informationssicherheit tragen und bei der Delegation von Aufgaben auch überprüfen kann.

Mit wieviel Aufwand ist bei den einzelnen Aufgaben zu rechnen?

Wie können sich die Personen aus- und weiterbilden?

Welche unabhängigen Stellen gibt es, welche die getroffenen Massnahmen überprüft? Wie oft muss dies erfolgen?

Dokument 8 - Schutzbedarfsfeststellung

Dokument 8:
**Schutzbedarfs-
feststellung**

- ✓ Überblick Dokument 8
- ✓ Selbständiges Durch-
gehen des Dokuments
- ✓ Fragen zum Dokument

Dokument 8 - Schutzbedarf feststellung

Was ist zu tun:

1. Liste der Fachanwendungen erstellen
2. Anwendungsverantwortlichen bestimmen
3. Schutzbedarf der Fachanwendungen (Vertraulichkeit/Integrität/Verfügbarkeit) festlegen

Zu Ziff. 2:

- 2.1 Interne Verantwortliche bestimmen (und auch dokumentieren)
- 2.2 Externe Verantwortliche dokumentieren (bspw. Auftragnehmende)
- 2.3 Datenstandort ermitteln und dokumentieren (intern/extern; falls extern: wo?)

Zu Ziff. 3:

- 3.1 Schutzbedarfskategorien ermitteln, überprüfen und allenfalls ergänzen
- 3.2 Feststellung Schutzbedarf der einzelnen Anwendungen betr. Vertraulichkeit, Verfügbarkeit und Integrität (anhand Schutzbedarfskategorien)
- 3.3 Überprüfen und anpassen

Dokument 8 - Schutzbedarfsfeststellung

Fragen

Welche Applikationen
muss ich alle auflisten?
Gehören dazu alle
Applikationen (Apps),
welche für den Unterricht
verwendet werden oder nur
diejenigen, welche auf die
Ebene Schule als
Organisation gehören?

Dokument 8 - Schutzbedarfsfeststellung

Fragen Datenklassifizierung

Wo ist diese eingebettet?

Wie muss die Nutzung eines E-Mail-Programms bezüglich der Datenklassifizierung erfassen?

Sicherheitsmassnahmen planen und umsetzen

Dokument 7 - Minimummassnahmenkatalog

Dokument 7:

Minimummassnahmen-
katalog

- ✓ Überblick Dokument 7
- ✓ Selbständiges Durch-
gehen des Dokuments
- ✓ Fragen zum Dokument

Sicherheitsmassnahmen planen und umsetzen

Dokument 7 - Minimummassnahmenkatalog

Dokument 7 - Minimummassnahmenkatalog

Was ist zu tun:

1. Sicherheitsmassnahmen den Verantwortlichen zuweisen (verantwortliche Mitarbeitende oder Auftragnehmende eintragen)
2. Basischeck: Status Massnahmen bestimmen und dokumentieren
3. Gap-Analyse (was ist vorhanden – was fehlt?)
4. Umsetzung planen; mit Termin, Priorität und Kosten
5. (Revision planen)

Sicherheitsmassnahmen planen und umsetzen

Dokument 7 - Minimummassnahmenkatalog

Fragen

Sind alle 149 Elemente Teil :
des
Minimummassnahmenkatal
ogs?

Sicherheitsmassnahmen planen und umsetzen

Dokument 7 - Minimummassnahmenkatalog

Dokument 7 - Minimummassnahmenkatalog

Prioritär

1. Weisungen für die Mitarbeitenden erstellen
2. Sensibilisierung der Mitarbeitenden planen
3. Rollen- und Berechtigungskonzept erstellen

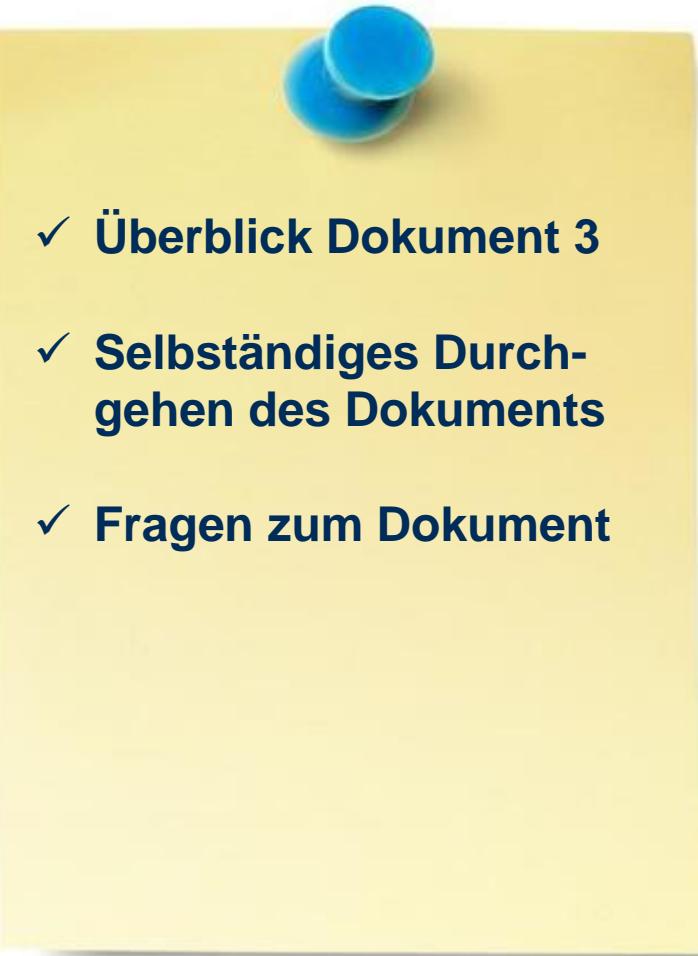
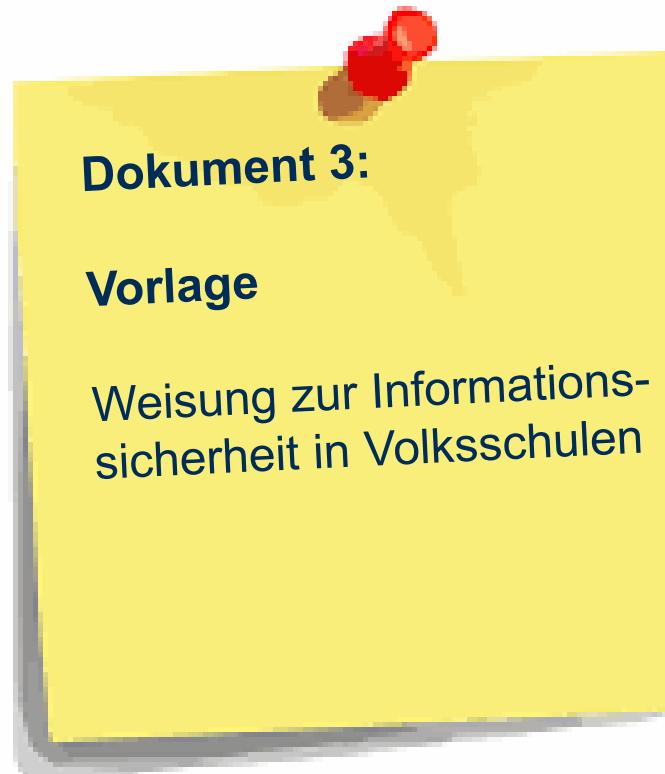
Kaffeepause

se von

0.30 Uhr

Dokument 3 – Vorlage: Weisung zur Informationssicherheit in Volksschulen

Informationssicherheit in Volksschulen



Dokument 3 – Vorlage: Weisung zur Informationssicherheit in Volksschulen

Was ist zu tun:

1. Überblick betreffend Inhalte der Vorlage für die Weisung verschaffen
2. Schritte 1 – 8 prüfen und für die konkrete Anwendung hin verwenden und erforderlichenfalls anpassen
3. Beschlussfassung durch die Schulpflege betreffend Leitlinie herbeiführen

Zu Ziff. 1-8: Einleitung/Geltungsbereich/Sicherheitsniveau (vgl. S. 3 ff.)

Text prüfen und auf konkrete Einrichtung hin ergänzen

Zu Ziff. 3.3: Datensicherung, -löschung und Entsorgung von Informationsträgern (vgl. S. 5)

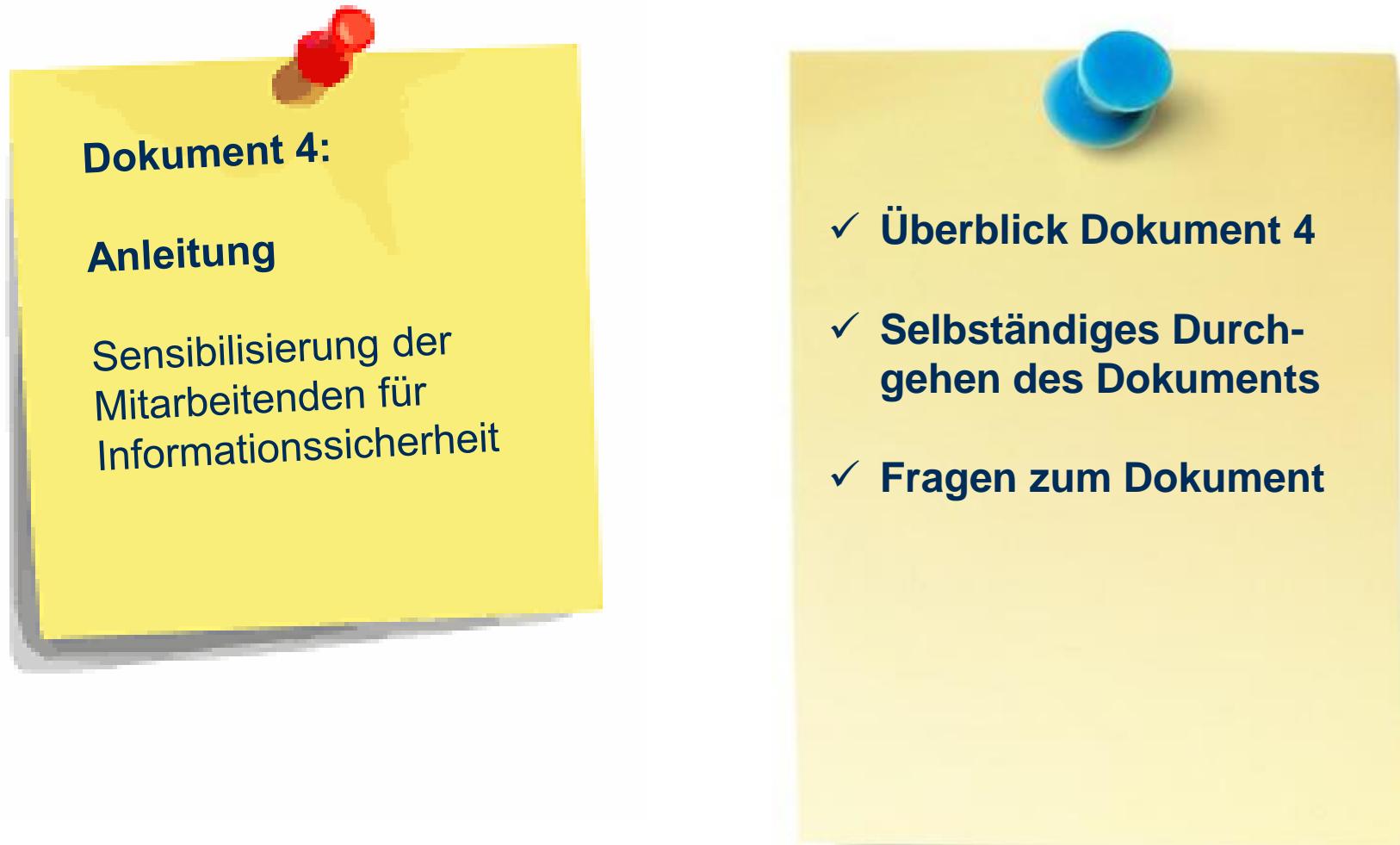
Prüfen, ob ggf. ein Löschkonzept bereits vorliegt oder noch erstellt werden muss.

Dokument 3 – Vorlage: Weisung zur Informationssicherheit in Volksschulen

Fragen

Wie wird mit BYOD von LP umgegangen? Was muss da beachtet werden?

Dokument 4 – Anleitung: Sensibilisierung der Mitarbeitenden für Informationssicherheit

- 
- Dokument 4:**
Anleitung
**Sensibilisierung der
Mitarbeitenden für
Informationssicherheit**
- ✓ **Überblick Dokument 4**
 - ✓ **Selbständiges Durch-
gehen des Dokuments**
 - ✓ **Fragen zum Dokument**

Dokument 4 – Anleitung: Sensibilisierung der Mitarbeitenden für Informationssicherheit

Was ist zu tun:

1. Überblick betreffend Inhalte der Anleitung zur Sensibilisierung verschaffen
2. Schritte 2 – 4 prüfen und für die konkrete Anwendung hin verwenden und erforderlichenfalls anpassen
3. Umsetzung veranlassen

Zu Ziff. 2: Planung (vgl. S. 2 ff.)

Inhalte prüfen und auf konkrete Einrichtung hin ergänzen/anpassen

Zu Ziff. 3: Umsetzung (vgl. S. 4 f.)

Modelle prüfen und auf konkrete Einrichtung hin ergänzen/anpassen

Zu Ziff. 4: Umsetzung (vgl. S. 5)

Korrekturmassnahmen und Verbesserungen kontinuierlich prüfen und vornehmen

Dokument 4 – Anleitung: Sensibilisierung der Mitarbeitenden für Informationssicherheit

Fragen

Wieviel Sensibilisierung der Mitarbeitenden ist genug, damit gesagt werden kann, dass wir genügend getan haben?

Müssen dazu alle Module geschult werden gemäss Anleitung?

Gibt es Materialien, welche für die Sensibilisierung verwendet werden können?

Dokument 5 - Vorlage: Rollen- und Berechtigungskonzept in Volksschulen

Dokument 5:

Vorlage

Rollen- und Berechtigungs-
konzept in Volksschulen

- ✓ **Überblick Dokument 5**
- ✓ **Selbständiges Durch-
gehen des Dokuments**
- ✓ **Fragen zum Dokument**

Dokument 5 - Vorlage: Rollen- und Berechtigungskonzept in Volksschulen

Dokument 5 - Vorlage: Rollen- und Berechtigungskonzept in Volksschulen

- Individuelle Vergabe führt zu Unübersichtlichkeit und grossem administrativem Aufwand ...
- Benutzern werden ihre Rollen zugeordnet; die Rollen enthalten Berechtigungen auf IT-Ressourcen
- Verschiedene Rollen können zu Gruppen zusammengefasst werden
- Eine einzelne Person kann mehrere Rollen innehaben

Dokument 5 - Vorlage: Rollen- und Berechtigungskonzept in Volksschulen

Ziele:

1. Klarheit bei der Vergabe von Rechten
2. Übergreifende, verbindliche Definition der Berechtigungsvergabe
3. Verringerung des administrativen Aufwands
4. Ermöglichung der Umsetzung des Verhältnismässigkeitsprinzips (need to know)

Dokument 5 - Vorlage: Rollen- und Berechtigungskonzept in Volksschulen

Beispiel aus anderem Zusammenhang:

Dokument 5 - Vorlage: Rollen- und Berechtigungskonzept in Volksschulen

Kann ich für die Zugriffsmatrix der Dateien von der Ordnerstruktur auf dem Server/Cloud ausgehen?

Was muss ich mir unter Rolle bei den Applikationen vorstellen?

Prozesse: da ist exemplarisch ein Prozess beschrieben. Dies sagt aber ziemlich wenig aus. Was ist das Ziel dieses Abschnitts?

Muss ich bei jeder Applikation aufschreiben, wer welche Zugriffsmöglichkeiten hat?
Bsp. Admin kann ..., Lehrperson kann...

Sind mit Mitgliedern die einzelnen Personen gemeint oder Personengruppen wie LP/Schulische Heilpädagogin etc.

Dokument 6 - Vorlage: Erklärung über die Nutzung von Internet und E-Mail/Informationssicherheit

Dokument 6:

Vorlage

Erklärung über die Nutzung von Internet und E-Mail sowie zur Informationssicherheit in Volksschule

- ✓ Überblick Dokument 6
- ✓ Selbständiges Durchgehen des Dokuments
- ✓ Fragen zum Dokument

Dokument 6 - Vorlage: Erklärung über die Nutzung von Internet und E-Mail/Informationssicherheit

Was ist zu tun:

1. Vorlage prüfen und für die konkrete Anwendung hin verwenden und erforderlichenfalls anpassen
2. Umsetzung veranlassen

Zu Seite 2: (Erklärung)

Inhalte prüfen und auf konkrete Einrichtung hin ergänzen/anpassen

Informationssicherheit – abschliessende Übersicht Dokumente

Für die Erstellung und Einführung der nötigen Leitlinien, Weisungen und Konzepte stehen folgende Dokumente zur Verfügung.

Dokumente

Leitfaden

Anleitungen

Vorlagen

Checklisten

Glossar / Abkürzungsverzeichnis

Thema

[Informationssicherheit in Volksschulen](#)

[Sensibilisierung der Mitarbeitenden für Informationssicherheit in Volksschulen](#)

[Erklärung zur Informationssicherheit in Volksschulen](#)

[Leitlinie zur Informationssicherheit in Volksschulen](#)

[Rollen- und Berechtigungskonzept in Volksschulen](#)

[Schutzbedarf feststellung Fachanwendungen in Volksschulen](#)

[Weisung zur Informationssicherheit in Volksschulen](#)

[Minimummassnahmenkatalog](#)

[Glossar und Abkürzungen Informationssicherheit](#)

Vielen Dank.

