Competence Center ICT VTGS
Autoren: Danny Frischknecht | Pascal Leuthold

Projekt: IT Referenzarchitektur

Version Mai 2025
CoC ICT des VTGS in Zusammenarbeit mit dem Amt für Volksschule des Kantons Thurgau

Inhaltsverzeichnis

1 Zielsetzung und Anforderungen 4
1.1 Sinn und Zweck dieser Empfehlungen 4
1.2 Körperschaften 4
1.3 Benutzergruppen 4
1.4 Gliederung der Referenz IT-Architektur 4
1.5 Funktionale Anforderungen 5
1.6 Nicht-funktionale Anforderungen 5
2 Basisinfrastruktur 6
2.1 Internetzugang 6
2.2 Telefonie 6
2.3 (Not-) Kommunikation 6
2.4 Sicherheitskonzept 7
2.5 Video - Überwachung 7
3 Netzwerkinfrastruktur 7
3.1 Wo? 7
3.2 USV 7
3.3 Switches 8
3.4 Netzwerke 8
3.5 Sicherheit im Netzwerk 10
3.6 Monitoring 11
4 Server und Speichersysteme 12
4.1 «on premise» 12
4.2 Cloud 12
4.3 Backup 13
4.4 Monitoring 13
5 Endgeräte 14
5.1 «Lifecycle» 14
5.2 Ausrüstung und Besitzverhältnisse 16
5.3 Mengengerüste und Finanzierung 18
5.4 Lehrpersonen 19
5.5 Kauf, Miete oder Leasing 22
5.6 Software 22
6 Präsentationstechnik 23

6.1 Pädagogik 23
6.2 Technik 23
6.3 Ökosystem 23
6.4 Im Detail 23
7 Drucker – Kopierer 24
8 Gerätemanagement 26
9 Software 27
9.1 Schulverwaltung (SVS) 27
9.2 «Notenverwaltung» und Kommunikation 27
9.3 Standardsoftware 27
9.4 Unterrichtssoftware 27
9.5 Spezialapplikationen 27
10 Datenarchitektur 28
10.1 Datenablage und Kollaboration 28
10.2 Datenschutz 28
10.3 Personendaten 28
10.4 Zugriffsmanagement und Berechtigungsstruktur 29
10.5 Datenverarbeitung und Verschlüsselung 30
11 Sicherheitsarchitektur 30
11.1 Benutzer-Authentifizierung 30
11.2 Firewalls und Netzwerksicherheit 30
11.3 web content screening 30
11.4 Datensicherheit und Backup 31
12 Support und Wartung 32
12.1 Technischer IT-Support 32
12.2 Pädagogischer Support 33
12.3 Supportfeedback / Evaluation 33
12.4 Vertrags- und Lizenzmanagement 34
12.5 Inventarisierung 35
13 Erweiterbarkeit und zukünftige Entwicklung 36
13.1 Skalierbare Infrastruktur 36
13.2 Trend Scouting 36
13.3 Umgang mit Updates und Upgrades 36
14 Begriffsklärungen und weiterführende Links 38

1 Zielsetzung und Anforderungen

1.1 Sinn und Zweck dieser Empfehlungen

Das vorliegende Dokument «Referenz IT - Architektur» wurde vom Kompetenzzentrum ICT (CoC-ICT*) des Verbands Thurgauer Schulgemeinden (VTGS*) erarbeitet.

Es beschreibt die Empfehlungen an die Informatik einer Schule im Kanton Thurgau. Damit sind Hard- und Software ebenso gemeint wie Dienste und Regelungen.
Die Empfehlungen erheben nicht den Anspruch auf Vollständigkeit, sie werden nach Bedarf aktualisiert. Im Dokument finden sich Verweise auf andere Dokumentationen des CoC ICT, welche stärker ins Detail gehen und tendenziell öfter aktualisiert werden.

Im Anhang findet sich ein Glossar mit Erklärungen zu Begriffen im Dokument sowie weiterführende Links zu gewissen Themen.

Auch diese können nach Bedarf ergänzt werden.

1.2 Körperschaften

Die Referenz IT*-Architektur kann auf alle drei Körperschaften (Primar-, Sekundar-, Volksschulgemeinde) angewendet werden.
Durch den Verbund der Körperschaften können allenfalls Synergien in der Ausgestaltung der IT-Architektur entstehen, beispielsweise durch den nahtlosen Übergang der Endgeräte von Schülerinnen und Schülern vom 2. bis zum 3. Zyklus.

1.3 Benutzergruppen

Die Referenz IT-Architektur bezieht alle Benutzergruppen einer Körperschaft mit ein. Es können folgende Benutzergruppen unterschieden werden:

- Lehrpersonen
- Schülerinnen und Schüler
- Schulleitungen
- Schulbehörde
- Schulverwaltung
- Mitarbeitende (Hausdienst, etc.)
- Eltern

1.4 Gliederung der Referenz IT-Architektur

Die Referenz IT-Architektur gliedert sich in folgende Themenschwerpunkte:

- Basisinfrastruktur
- Netzwerkinfrastruktur
- Server und Speichersysteme
- Endgeräte
- Software
- Datenarchitektur
- Sicherheitsarchitektur
- Support und Wartung
- Erweiterbarkeit und zukünftige Entwicklung

1.5 Funktionale Anforderungen

An die Informatik einer Körperschaft werden im Übergeordneten folgende funktionalen Anforderungen gestellt.

- Unterstützung des Lernens durch eine adäquate Infrastruktur
- Medien- und Informatikbildung auf dem neusten Stand der Technik
- Sicherstellung des Zugangs zu Lern- und Standardsoftware für verschiedene Fächer
- Kommunikation über alle Benutzergruppen
- Administrationslösung zur Schulorganisation und zur Verwaltung von Schüler- und Lehrerdaten

1.6 Nicht-funktionale Anforderungen

An die Informatik einer Körperschaft werden im Übergeordneten folgende nicht-funktionale Anforderungen gestellt.

- Skalierbarkeit, Anpassbarkeit der Infrastruktur an die Anzahl der Benutzer
- Zuverlässigkeit, Minimierung von Ausfallzeiten, insbesondere in Unterrichtszeiten
- Sicherheit von Daten und Infrastruktur
- Erfüllung der gesetzlichen Anforderungen zum Datenschutz und weiteren Vorschriften, insbesondere im Hinblick auf den Schutz von Personendaten

2 Basisinfrastruktur

Im Kapitel Basisinfrastruktur werden Komponenten der Referenz IT-Architektur beschrieben, welche für den reibungslosen Betrieb einer Körperschaft grundlegend sind.

2.1 Internetzugang

Die Ansprüche der Infrastruktur in Schulen auf breitbandige Internetzugänge, nehmen stetig zu und verändern sich.

Viele Dienste sind cloudbasiert* oder können cloudbasiert administriert und überwacht werden (Schliessanlagen, Videoüberwachung, Telefonie etc.).

Schulen benötigen eine stabile, leistungsfähige Verbindung ins Internet. Das ist im Idealfall eine Glasfaser - Mietleitung (LWL*) mit einer garantierten Bandbreite von mindestens 1 GBit/s*.
Das sind sogenannt «gemanagte Business-Lösungen»*, welche nicht dem «best effort» Prinzip* unterworfen sind.

Ein zweiter Zugang als Redundanz* über einen anderen Anbieter wird empfohlen, dieser kann mit reduzierter Bandbreite ausgestattet sein.

2.2 Telefonie

Durch den Übergang von analoger zu digitaler Technologie (IP-Telefonie*) haben sich die Möglichkeiten verändert.

Meist kann auf eigentliche Telefonanlagen verzichtet werden, verschiedenste Telefone und Kommunikationsmedien wie Computer, Tablet oder Smartphone können integriert werden.

Eine weitere Veränderung; zu den klassischen Telefonie-Supportern (Elektriker) kommen «normale» IT-Dienstleister hinzu, was für Schulen die Reduktion von Schnittstellen bedeuten kann.

Die Telefonie kann folgende Komponenten umfassen:

1. Eigene Telefonanlage mit Geräten
2. Eigene Telefonanlage mit Softclient* (Programm, App) auf dem Computer
3. Outsourcing der gesamten Telefonanlage, Softclient (Programm, App) auf dem Computer
4. Videotelefonie (Teams, Zoom etc.)

2.3 (Not-) Kommunikation

Zur Not-Kommunikation gehören Gefahrenmelder für Brand, Rauch, Gas und Wasser gleichwohl wie auch Notrufe aus Liftanlagen, IV Toiletten oder Turnhallen.

Über entsprechende Schnittstellen kann es auch Sinn machen, Themen wie Evakuierungs- und Durchsagesysteme, Technische Gebäudealarme, alarmierte Notausgänge und weiteres in der Kommunikationslösung der Schule aufzugreifen. Solche Integrationen sind periodisch auf ihre Funktionsfähigkeit zu testen. Sämtliche Tests sind zu dokumentieren. Dieses Kapitel ist in der Regel im Sicherheits- und Notfallkonzept der Schule dediziert beschrieben und abgehandelt.

2.4 Sicherheitskonzept

Der Kanton Thurgau stellt den Schulen Unterlagen für ein Sicherheitskonzept zur Verfügung:
https://av.tg.ch/themen/sicherheit-in-schulen.html/13464

2.5 Video - Überwachung

Eine Video-Überwachung ist ausschliesslich unter Bewilligung durch die Schulbehörde zu installieren. Dabei sind die gesetzlichen Anforderungen bezüglich des Datenschutzes* einzuhalten.

Besonders auf die Speicherung und Aufbewahrung der Daten ist zu achten, sie soll zwar möglichst kurz sein, muss jedoch den Ansprüchen der Schule genügen (Wochenende, Ferien).

Der Einsatz einer Videoüberwachung muss so gekennzeichnet werden, dass die Betroffenen vor dem Betreten des überwachten Bereiches informiert werden.

Der Vorgang zur Löschung der Daten sollte definiert und automatisiert werden.

3 Netzwerkinfrastruktur

Die Netzwerkinfrastruktur beschreibt die Hardware zur Vernetzung der Standorte, die Verkabelung eines Standorts, das WLAN*, die Überwachung der Zugänge durch Firewalls*, das Monitoring* sowie die Sicherheit aller Räume und Systeme.

3.1 Wo?

Für die Netzwerkinfrastruktur müssen sinnvolle Räume und Aufbewahrungsorte zur Verfügung stehen und entsprechend geschützt werden. Bei «on premise»* Serverinfrastruktur ist das aufwendiger, quantitativ wie qualitativ.

Serverräume müssen mit einer Zugangskontrolle versehen sein, die idealerweise ins Schliesssystem integriert ist.

Zudem müssen sie nach Bedarf klimatisiert werden und vor Brand oder Wassereinbruch geschützt sein.

Auch Racks* für Server, Firewall, USV oder Netzwerkkomponenten, zum Beispiel Switches* müssen abgeschlossen sein, der Zugang soll auf möglichst wenige Personen beschränkt werden.

Je nach Grösse und Komplexität einer Anlage sollte eine Redundanz* ins Auge gefasst werden.

3.2 USV

Eine «Unterbrechungsfreie Stromversorgung»* (USV) ist zwar «nur eine Batterie», allerdings eine intelligente. Sobald der Strom ausfällt, übernimmt die USV die Versorgung. Damit werden kurze Unterbrüche überbrückt, bei längeren Unterbrüchen werden die Systeme sauber heruntergefahren.

Somit ist dieses unscheinbare Gerät sehr zentral für die Sicherheit eines Netzwerkes.

Die Leistung der USV muss dem Bedarf entsprechen, die Funktion regelmässig überprüft werden.

3.3 Switches

Die Standorte der IT-Verteiler ergeben sich aus den spezifischen Bedürfnissen und den örtlichen Gegebenheiten (Anzahl Tertiäranschlüsse, Maximaldistanz zwischen Schrank und Kommunikationssteckdose von 90 m, Zugang zu den Installationsmedien).
Die Aktivkomponenten wie Switches sind mit gesicherter Stromversorgung und geeigneter Lüftung in Racks zu platzieren und vor physischem Zugriff zu schützen.

Wichtig ist, dass Switches PoE (power over ethernet) unterstützen, also die Stromversorgung von WLAN-Acces Points* direkt über das Netzwerk.

3.4 Netzwerke

3.4.1 Topologie

Es gibt verschiedene Möglichkeiten, um Kabelnetzwerke aufzubauen. Zudem gibt es verschiedene Ansprüche an solche Netzwerke.

Verschiedene Gebäude an einem Standort oder gar Standorte untereinander können vernetzt werden. Was Sinn macht und welchen Aufwand es bedeutet, sollte mit Fachleuten geklärt werden.

Gegebenefalls ist es sinnvoll, einen Hauptstandort mit der zentralen Infrastruktur zu erstellen und die Aussen-Standorte als schul-internes Netzwerk zu erschliessen.

Heute werden Netzwerke «sternförmig» aufgebaut. Das bedeutet, dass zwischen der zentralen Verteilung (Switch) und jeder Netzwerksteckdose ein eigenes Kabel geführt wird. Fällt eine Verbindung aus, betrifft es nur diese eine Dose.

3.4.2 WAN

Das «wide area network» verbindet Gebäude an geografisch unterschiedlichen Orten. Das können zum Beispiel verschiedene Schulstandorte sein.

Solche WAN-Netzwerke sind aufwendig und meist eher teuer. Sie machen nur Sinn, wenn ein Telekom- oder Netzwerkanbieter diese Verbindungen erstellt oder besitzt, und vermietet.

Eine Beratung durch Fachleute ist unabdingbar.

3.4.3 LAN

Das «local area network», das interne Kabelnetzwerk, ermöglicht Verbindungen zwischen verschiedenen Gebäuden oder innerhalb eines Gebäudes.
Solche Kabelnetzwerke können entweder mit Kupferkabeln (Ethernet*) oder mit Glasfaserkabeln (Lichtwellenleiter*) realisiert werden.

Dabei sind Glasfaserkabel leistungsfähiger und können längere Distanzen überwinden. Im Anhang findet sich eine ausführliche Zusammenstellung über Standards und Datendurchsatz.

Vereinfacht kann gesagt werden; Gebäude untereinander müssen mit Glasfaser vernetzt werden, gebäudeintern reichen Ethernetkabel meist aus.

Kabelgebundene Netzwerke müssen bei der Erstellung oder der Aktualisierung mit einer Software ausgemessen werden. Diese Ausmessung und Protokollierung sollte regelmässig aktualisiert werden.

3.4.4 WLAN

WLAN-Netzwerke* werden zunehmend wichtiger. Praktisch alle Clientgeräte kommunizieren über das Funknetz. Zudem nimmt die Anzahl webbasierter Lernplattformen zu, Datenablagen und Kommunikation funktionieren über das Internet, da sie in der Cloud* liegen.

In der Industrie ist es schon länger üblich, in den Schulen nimmt es zu; die Geräteverwaltung und -administration über WLAN. Das betrifft nicht nur Computer und Tablets, sondern auch Drucker und Kopierer, Schliessanlagen, Telefonie, Alarmierung etc.

Beim Aufbau eines WLAN Netzes gilt die Regel; in jedem Raum, in welchem Endgeräte genutzt werden, wird ein Access Point (AP) installiert. Das bedeutet mehr Leistung und gleichzeitig niedrigere Strahlungswerte, da die einzelnen APs weniger Fläche abdecken müssen.

Technisch sollen die WLAN-Komponenten den WLAN Standard Wifi 6* unterstützen (Stand 2025) und mit MIMO-Technologie* funktionieren. Nur so können tatsächlich mehrere Zugriffe gleichzeitig bearbeitet werden.

Ebenfalls einen Einfluss auf die Leistungsfähigkeit hat die Positionierung der APs. Im Idealfall werden sie mittig an der Decke positioniert, da sie kugelförmig strahlen. Das hat einen Einfluss auf das Setzen der entsprechenden Anschlussdosen.

Die Stromversorgung sollte direkt über das Netzwerk geschehen (poe – power over ethernet), damit keine Stromanschlüsse notwendig sind.
Im Idealfall geschieht das durch entsprechend Switches, möglich ist es auch mit Adaptern, welche zwischen Switch und Anschlussdose montiert werden.

3.4.5 Abdeckung und Bandbreite

Die Abdeckung und Bandbreite (Geschwindigkeit) bei WLAN-Netzwerken kann mit sogenannten Site Surveys* festgehalten werden. Das sind Nutzungssimulationen, welche die Abdeckung grafisch aufzeigen.

Eine einfache, Möglichkeit eines «Site Survey» ist, die einzelnen Standorte mit einem Laptop abgehen und prüfen,ob das Netz überall stark genug ist und die automatische Weiterleitung zwischen den Teilnetzwerken funktioniert.

3.5 Sicherheit im Netzwerk

3.5.1 Struktur

Die Netzwerke können entlang der Benutzergruppen (Schülerinnen und Schüler, Lehrpersonen, Schulverwaltung und Schulleitungen, Schulbehörde und Mitarbeiter) zur Erhöhung der Sicherheit und Vertraulichkeit voneinander getrennt werden (Segmentierung). Diese Trennung wird softwaremässig ausgeführt.

Die Netzwerkstrukturen sollen dabei jedoch flach, ohne unnötige Hierarchien und robust ausgelegt sein. Welche Struktur im Einzelfall Sinn macht, sollte mit Fachleuten besprochen und definiert werden.

3.5.2 Schutz

Netzwerke sollen durch entsprechende Massnahmen geschützt werden, in erster Linie durch Firewalls, aber auch durch sinnvolle Nutzereinbindung und den Verzicht auf unsichere Technologien.

3.5.3 Identifikation / Authentifizierung

Es soll gewährleistet werden, dass Lehrpersonen, Mitarbeitende und nach Bedarf Schülerinnen und Schüler automatisch auf die Netzwerke an den einzelnen Standorten zugreifen können.

Damit die Zugriffe sicher sind, gibt es verschiedene Möglichkeiten.

- Nutzername und Passwort
- Mac-Adresse* des Gerätes
- Voucher*

Das Einloggen über Nutzername und Passwort ist mühsam, besonders für Computer, welche durch verschiedene Personen eingesetzt werden.

Voucher machen für den temporären Einsatz Sinn, also etwa für Gäste oder Praktikantinnen und Praktikanten.

Die sicherste Möglichkeit ist das Einbinden der Mac-Adresse. Das ist eine Art individuelle, einmalige Seriennummer, die jedes netzwerkfähige Gerät besitzt.

Diese Adressen können zentral erfasst und dann im Netzwerk freigegeben werden. So ist keine Anmeldung mehr notwendig.

Beim Einsatz von schuleigenen und privaten Geräten (Handys Lehrpersonen…) macht die Kombination aus Benutzername/Passwort sowie Mac-Adresse Sinn.

3.5.4 Zugänge

Nach wie vor werden bei lokalen Serverinfrastrukturen sogenannte VPN-Zugänge* genutzt. Diese vermitteln ein Gefühl von Sicherheit, weil ein privater Tunnel zwischen Server und Endgerät hergestellt wird.

Diese Sicherheit ist allerdings relativ, denn auch VPN-Zugänge können gehackt werden, und sind nur so zuverlässig, wie Nutzerinnen und Nutzer mit ihren Zugangsdaten umgehen. Oft bleiben VPN-Tunnel an Clientgeräten «aus Bequemlichkeit» geöffnet.

Dabei gilt es, die Haltung, Verwaltung und Sicherheit von Daten zu regeln und Zugriffe klar festzulegen. Gesicherte Cloud-Zugänge sind dabei für die Mehrheit der Nutzer sicherlich genügend.

3.5.5 Firewall

Die gesamte IT Infrastruktur wird über Firewalls - möglichst redundant - vor Angriffen, Schadsoftware, Datenverlust und unautorisierten Zugriffen geschützt.

Firewalls sollten von innen und gegen aussen so geschlossen wie möglich sein, erlaubte Zugriffe sind explizit zu definieren und entsprechend zu konfigurieren.

Hinweis; Firewalls benötigen teils viel Bandbreite, insbesondere für Internetfilter (web content screening). Es lohnt sich, bei der Firewall nicht zu sparen. Eine grosse Performance hilft für die Sicherheit und ist nachhaltiger, weil die Ansprüche laufend steigen.

Zentral beim Einsatz von Firewalls ist die erwähnte Inhaltsprüfung (web content screening). Sie verhindert Zugriffe auf jugendgefährdende Inhalte wie Gewalt, Pornographie, Rassismus etc..

3.6 Monitoring

Sämtliche Komponenten des Netzwerks (Firewall, Switch, WLAN etc.) werden proaktiv und möglichst automatisiert überwacht. Bei Fehlverhalten werden entsprechende Meldungen abgesetzt und durch den internen oder externen Support bearbeitet.

4 Server und Speichersysteme

Server* und Speichersysteme können «on premise», also lokal in der Schule betrieben, oder in ein externes Rechenzentrum (Cloud) ausgelagert werden.

Beide Systeme sind zugelassen und je nach Situation sinnvoll. Der Entscheid sollte auf Kriterien basieren, die einen sinnvollen Umgang, genügend Sicherheit und vernünftige Ressourcen gewährleisten.

Es lohnt sich, das Dafür und Dawider genau abzuwägen.

4.1 «on premise»

Die Server und Speichersysteme werden am Standort der Schule betrieben. Die Vernetzung weiterer Standorte erfolgt von diesem zentralen Punkt aus.

Server können gekauft, geleast oder gemietet werden. Es empfiehlt sich, sie zu virtualisieren*. Die Benutzer mit Zugriff sind zu definieren und auf ein Minimum zu reduzieren.

Serverdienste sind entsprechend der zu betreibenden Softwarelösungen und der Anzahl Benutzerinnen und Benutzer auszulegen. Kritische Server (Backup, Recovery*…) sind redundant an zwei örtlich voneinander getrennten Standorten zu betreiben.

Lokale Serverinfrastruktur macht Sinn, wenn es spezielle, dringend benötigte Dienste braucht, die lokal installiert sein müssen.

An Serverräume müssen gewisse Anforderungen gestellt werden

- Sie müssen abschliessbar und mit einer Zutrittskontrolle versehen sein.
- Sie müssen vor Wassereinbruch und Brand geschützt sein.
- Eine angemessene Kühlung und Entfeuchtung müssen vorhanden sein.
- Die Racks (Serverschränke) sind gross genug auszulegen und müssen ebenfalls abschliessbar sein.

Wird eine lokale Datenablage als notwendig erachtet, kann das auch mit minimaler Infrastruktur (NAS*) gelöst werden.

Lokale Serverinfrastruktur ist kostenintensiv, braucht viel Unterhalt und KnowHow und ist im Normalfall weniger sicher als externe Rechenzentren, da diese in denselben Zentren Hunderte oder Tausende andere Kunden betreuen.

4.2 Cloud

Die Server und Speichersysteme werden in einer Cloud, also einem externen Rechenzentrum betrieben. Das können auch unterschiedliche Cloudsysteme oder -anbieter sein, etwa mit unterschiedlichen Ansprüchen an Sicherheit und Datenschutz.

Die Server und Speichersysteme sollen aufgrund der datenschutzrechtlichen Bestimmungen in Rechenzentren der Schweiz betrieben werden.

Die Datenübertragung von den Standorten der Schule bis in das Rechenzentrum des externen Partners muss verschlüsselt erfolgen. Das ist bei den meisten Anbietern gewährleistet, sie ist standardmässig 256 Bit TLS* verschlüsselt. Zusätzliche Verschlüsselungen sind möglich, machen aber nur Sinn (Aufwand, Verhältnismässigkeit…) wenn sehr sensible Daten gespeichert werden sollen.

Es gibt verschiedene Ansprüche an Verfügbarkeit, Zuverlässigkeit, Redundanz, Security*, etc. an die Partner und Rechenzentren. Je höher die Ansprüche, desto höher sind die Kosten, der Anstieg ist teils exponentiell.

Es macht Sinn, adäquate Normen und Ansprüche zu definieren, welche den tatsächlichen Bedürfnissen der Schulen entsprechen.

Auch hier gilt, der Beizug von Fachleuten lohnt sich.

4.3 Backup

Kritische Daten, sowohl lokal als auch in der Cloud, sind periodisch nach definierten Regeln zu sichern.

Bei lokalen Datenablagen sind die Daten auf einem passenden Medium automatisiert zu speichern (Festplatte, Bandsysteme). Die Medien sind an einem anderen geografischen Standort aufzubewahren. Die Widerherstellung der Daten aus dem Backup ist regelmässig zu testen.

Bei Daten in der Cloud kann ein Backup ebenfalls Sinn machen, lokal oder in einer anderen Cloud.

Die Ansprüche an ein solches Backup müssen diskutiert und definiert werden, sie unterscheiden sich von Schule zu Schule (Risikobeurteilung).
Viele Datenverluste sind relativ leicht zu verschmerzen (Schülerarbeitsblatt, Elternbrief etc.), die Sensibilisierung der Mitarbeitenden ist oft sinnvoller und kostengünstiger als teure technische Lösungen.

Die Verantwortung für Backups kann auch ganz oder teilweise an die Nutzerinnen und Nutzer delegiert werden.

Manche Schulen verzichten vollständig auf Backups, weil sie dem Anbieter der Cloudlösung vertrauen.

So sieht etwa die Backuplösung von Microsoft 365 aus

- *Die Daten werden regelmässig gesichert, eine Redundanz zwischen mehreren Rechenzentren ist gewährleistet.*
- *Werden Daten versehentlich gelöscht, können sie bis zu 90 Tage selbständig oder durch den lokalen Admin wieder hergestellt werden.*
- *Nach diesen 90 Tagen kann eine Wiederherstellung durch MS gemacht werden (kostenpflichtig). Erfahrungsgemäss ist das sehr selten und lohnt sich nur bei sehr wichtigen Daten.*

4.4 Monitoring

Sämtliche Komponenten des Server- und Speichersystems werden proaktiv und automatisiert überwacht.

Dabei gilt einmal mehr; ein seriöses und professionelles Monitoring ist anspruchsvoll und schnell kostenintensiv.

Bei Clouddiensten übernimmt der Anbieter des Rechenzentrums ein solches Monitoring.

5 Endgeräte

Unter Endgeräten (Clients) sind alle Geräte zu verstehen, mit welchen die Benutzergruppen in Kontakt kommen. Sämtliche Endgeräte sind einem Lebenszyklus unterworfen und dementsprechend zu ersetzen.

Endgeräte können ebenfalls gekauft, geleast oder gemietet werden.

5.1 «Lifecycle»

Schulen müssen ein Interesse haben, dass Geräte nachhaltig genutzt werden. Eine durchdachte Wahl der Geräte (Qualität, Ausstattung) kann die Einsatzdauer signifikant verlängern.

Es gibt beim Ersatzzyklus zwei Faktoren, erstens die «theoretische, technische» Lebensdauer, zweitens die «effektive» Einsatzdauer.

Technisch gelten etwa folgende Richtwerte für den Livecycle*

- Tablets je nach Hersteller und Qualitätsstufe drei bis vier Jahre
- Laptops je nach Hersteller und Qualitätsstufe vier bis fünf Jahre
- Desktopgeräte je nach Hersteller und Qualitätsstufe fünf bis sechs Jahre

Die effektive Einsatzdauer in Schulen liegt meist beim empfohlenen Maximum oder darüber. So sind Tablets oder Laptops oft fünf bis sechs Jahre im Einsatz, Desktops teilweise bis acht Jahre.

Entscheidende Faktoren sind meist nicht, wie lange die Geräte physisch funktionieren, sondern

- Wie lange kann Software aktualisiert werden, besonders Betriebssysteme oder Standardsoftware?
  Solange Sicherheitsupdates möglich sind und auf aktualisierte Programme oder Betriebssysteme verzichtet werden kann, können Geräte eingesetzt werden.
- Weitere Faktoren sind Netzteile oder Akkus.
  Sie haben eine beschränkte Lebensdauer und ihr Ersatz ist oft unverhältnismässig teuer.
- Qualitativ hochwertige Geräte haben weniger Schwachstellen an der Hardware (Anschlüsse, Gelenke, Bildschirm), sind aber meist teurer.
- Die Ausfall- oder Reparaturkurve verändert sich mit dem Alter – sie steigt zunehmend steil an. Diese Kostensteigerungen haben ebenfalls einen Einfluss auf die Einsatzdauer.
- Werden Geräte ersetzt, wird der Gerätepark heterogener. Das bedeutet mehr und aufwendigeren Support.

Die Lebensdauer von Geräten kann zudem verlängert werden, wenn sie nach dem Einsatz in Schulen einem Wiederverkauf (Remarketing Pt. 5.1.1) zugeführt werden. Sie erhalten ein «zweites Leben» und erhöhen damit die Nachhaltigkeit.

5.1.1 Weiterverwendung nach Ausmusterung in der Schule

In der Schweiz stellen wir hohe Ansprüche an die Infrastruktur. Was bei uns ausser Betrieb genommen wird, kann unter Umständen anderswo noch länger eingesetzt werden.

Dazu gibt es verschiedene Möglichkeiten

- Weitergabe innerhalb der Schule.
  Die Idee ist auf den ersten Blick bestechend, in den meisten Fällen aber mit viel Aufwand und Ärger verbunden:
  - Die Geräte müssen sicher gelöscht und mit Leerdaten überschrieben werden. Schulen haften, wenn Software oder Daten auf den Geräten verbleiben, die nicht lizenziert sind oder da nicht hingehören.
  - Die Geräte müssen aufbereitet (refurbished) werden (Netzteile, Kabel, Adapter…
  - Die Abnehmerinnen und Abnehmer erwarten Support oder Garantieleistungen, auch wenn diese ausbedungen werden.
  - Der Verkauf ist administrativ aufwendig und für die Verwaltungen oft mit Ärger verbunden (Zahlungsmoral…)
  - Der Verkaufserlös deckt die Aufwände praktisch nie.
  - Die Nachfrage ist meist bescheiden, besonders wenn die Geräte in der Schule schon lange im Einsatz waren.
- Professioneller, externer Wiederverkauf – «Remarketing»
  Es gibt spezialisierte Unternehmen, welche Hardware zurücknehmen, nach hohen Standards sicher löschen und wieder aufbereiten, weiterverkaufen oder zumindest korrekt entsorgen.
  Das hat für die Schule viele Vorteile.
  - Sie haben kaum Aufwand.
  - Eine sinnvolle Nachhaltigkeit ist gewährleistet.
  - Die sichere Löschung, Aufbereitung und Entsorgung werden gegenüber den Schulen durch Zertifikate garantiert.
  - Schulen wissen, in welche Märkte die Geräte geliefert werden.
  - Es gibt oft eine Refinanzierung – natürlich abhängig von Hersteller, Zustand und Alter der Geräte.
- Für den Weitergabe an Lehrpersonen oder Schülerinnen und Schüler können Onlineshops ausschliesslich für die Schule eingerichtet werden. Die Abwicklung erfolgt dann über die Remarketingfirma.

5.1.2 Abschreibung vs «Lifecycle»

Schulen haben Vorschriften, über welchen Zeitraum sie abschreiben müssen, nach HRM2 sind das vier Jahre. Bei der Abschreibung handelt es sich aber nur um eine buchhalterische Wertbereinigung, sie hat keinen Einfluss auf den Geräteersatz.

Die Abschreibungsfrist hat demnach nichts mit dem Ersatzzyklus zu tun, selbst wenn Schulen diese Fristen zugrunde legen.

5.2 Ausrüstung und Besitzverhältnisse

Bei der Nutzung von Clientgeräten in der Schule gibt es eine grosse Spanne zwischen dem Einsatz privater Geräte von Lehrpersonen und verwalteten Geräten der Schülerinnen und Schüler oder der Mitarbeitenden.
Dabei müssen einige Benennungen definiert und unterschieden werden.

5.2.1 «byod»

«Bring Your Own Device» meint, dass Schülerinnen und Schüler eigene, private Geräte mitnehmen und nutzen dürfen. Solche Systeme sind in Schulen kaum mehr anzutreffen, Aufwand und Nutzen stehen in einem krassen Missverhältnis.

Es hat sich gezeigt, dass mehr neue Probleme entstehen als alte gelöst werden, zudem werden kaum Kosten eingespart.

Die Schulen sind mit Sicherheits- und Haftungsfragen konfrontiert, müssen teils komplexe technische Aufgaben bewältigen und Lehrpersonen müssen unterschiedliche Systeme und Applikationen betreuen.

Das Modell gibt es heute noch an Mittel- Berufs- und Hochschulen. Den Studierenden werden aber detaillierte Vorgaben gemacht, welche Bedingungen die Geräte erfüllen müssen und der schulinterne Support ist sehr eingeschränkt.

Zudem müsste gefordert werden, dass die Geräte den Anforderungen der Schule entsprechen (technische Leistungsvorgaben).

5.2.2 Private Geräte

Das Gerät gehört der entsprechenden Person, ist nicht Teil der Schulinfrastruktur und kann nicht oder nur bedingt durch die Schul-IT verwaltet werden. Trotzdem erhalten Lehrpersonen den Zugang zum Internet und der zentralen Datenablage.

5.2.3 Computerräume

An Schulen machen dedizierte Informatikschulzimmer nur noch bedingt Sinn. Halbklassensätze oder one2one-Ausstattungen sind flexibler und meist kostengünstiger, besonders, weil kein spezieller Raumbedarf besteht.

Falls Computerräume benötiget werden, sollten sie flexibel gestaltet und ausgestattet werden.
So sollten eher Laptops, Convertibles oder Tablets anstelle von Desktopcomputern eingesetzt werden. Es können auch Arbeitsplätze mit Dockingstationen, externen Bildschirmen und Tastaturen oder anderer Peripherie ausgestattet sein, an welche die Nutzerinnen und Nutzer direkt ihre persönlichen Geräte anschliessen.
So können auch spezielle Bedürfnisse (Kurse für Musik, Multimediaanwendungen, Bildbearbeitung…) abgedeckt werden.

5.2.4 Poolgeräte

Diese Computer gehören der Schule, werden aber von verschiedenen Personen genutzt. Sie sind üblicherweise restriktiv verwaltet und nur teilpersonalisiert. Teilpersonalisiert meint, dass die Geräte alle verwaltet und identisch aufgesetzt sind, dass Schülerinnen und Schüler aber über Accounts (Zugänge, Nutzerprofile). auf ihre persönlichen Produkte und Ablagen zugreifen können

5.2.5 Persönlich

Die Geräte gehören ebenfalls der Schule, werden aber personalisiert, also einem bestimmten Nutzer oder einer bestimmten Nutzerin zugeteilt.

Bei Lehrpersonen kann das bedeuten, dass die Geräte mit Administrationsrechten versehen sind, auch private Software installiert und das Gerät ausserhalb des Schulnetzes genutzt werden kann.

Bei Schülerinnen und Schülern kann es bedeuten, dass die Geräte in einem bestimmten Rahmen persönlich konfiguriert und ebenfalls ausserhalb der Schule genutzt werden können. In diesem Kontext spricht man dann auch von «one2one».

Die Nutzung persönlicher Geräte sollte von Schulen reglementiert werden. Es muss klar sein, was man innerhalb und teilweise ausserhalb der Schule darf und was nicht.

Dabei müssen Sicherheit und Datenschutz ein hohes Gewicht haben und Missbräuche so weit als möglich verhindert werden. Nicht ausser Acht gelassen werden dürfen Haftungsfragen (Schülerinnen und Schüler, Eltern…).

Das gilt nicht nur für Schülerinnen und Schüler, sondern auch für Lehrpersonen, Schulleitung, Schulbehörde und alle anderen Mitarbeitenden.

5.2.6 Ersatzgeräte

Einige Schulen beschaffen mehr Geräte, als sie aktuell benötigen. Diese Geräte können als Ausgleich für unerwartete Veränderung der Anzahl Nutzenden eingesetzt werden, als Ersatz bei Ausfall oder Reparaturen oder für temporäre Mitarbeitenden (Praktikantinnen und Praktikanten, Gäste).

Für Ausfall und Reparaturen macht es unter Umständen mehr Sinn, mit dem externen Anbieter im Dienstleistungsvertrag eine Vereinbarung zu treffen, damit ein schneller Austausch oder Ersatzgeräte durch den Anbieter gewährleistet werden.

Temporäre Mitarbeitende oder Gäste verfügen oft über eigene Geräte, ein Zugang zum Internet und allenfalls auf eine Datenablage reicht oft aus.

5.2.7 Nutzung ausserhalb der Schule

Computer von Lehrpersonen werden innerhalb und ausserhalb der Schule genutzt. Das gilt teilweise auch für Laptops oder Tablets von Schülerinnen und Schülern.

Dazu braucht es:

- Richtlinien für die Nutzung von Geräten für die Lehrpersonen und die Lernenden sowie eine Klärung der Haftungsfrage bei Beschädigung, Verlust oder Diebstahl
- Internetfilter (web content screening) auf Schülerinnen- und Schülergeräten, der auch ausserhalb des Schulnetzes aktiv ist
- Aktueller Virenschutz auf sämtlichen Geräten

5.3 Mengengerüste und Finanzierung

5.3.1 Schülerinnen und Schüler

Aktuell sehen die Ausrüstungen in Schulen etwa so aus (Stand 2025):

- Kindergarten zwei bis vier Tablets pro Abteilung
- Klassen 1 bis 4 Poolgeräte, allenfalls personalisiert, sinnvollerweise ein Halbklassensatz pro Abteilung
- ab 5. Klasse «one2one» Ausrüstung der Schülerinnen und Schüler mit personalisierten Geräten. Eine «one2one» Ausrüstung ist auch ab der dritten oder vierten Klasse denkbar, sollte aber gut abgewogen und diskutiert werden.
- Auf der Sekundarstufe eine «one2one» - Ausstattung. Üblicherweise sind die Geräte personalisiert und können ausserhalb der Schule genutzt werden.

Vom Kindergarten bis und mit vierter Klasse sollten Tablets vorgezogen werden, da sie leichter, flexibler und robuster sind als Laptops, ihre Leistung und Funktionalität ist oft besser. Zudem sind die Einflussmöglichkeiten auf das Betriebssystem oder Programme schwieriger, die Geräte sind also sicherer.

In der fünften und sechsten Klasse können sowohl Tablets als auch Laptops/Convertibles* Sinn machen. Das hängt von der Philosophie der Schule ab.

Dasselbe gilt für Sekundarschulen. Dort sind tendenziell häufiger Tablets im Einsatz.

Bei Laptops ist auf Gewicht, Grösse und Robustheit zu achten, besonders, wenn sie ausserhalb der Schule genutzt werden dürfen. Zudem sollten Transporthüllen (Sleeves, Cases) beschafft werden.

5.4 Lehrpersonen

Die Anforderungen an die Ausrüstung von Lehrpersonen haben sich in den letzten Jahren verändert.

Desktoprechner am Arbeitsplatz waren früher praktisch, weil damit auch Infrastruktur wie Visualizer, Display oder Beamer sowie Audioanlagen gesteuert wurden.

Heute arbeiten Lehrpersonen mobiler, dieselben Räume werden oft von verschiedenen Menschen genutzt.
So werden weitgehend Laptops, seltener Tablets eingesetzt, oft kombiniert mit Dockingstationen und grossen Bildschirmen am Arbeitsplatz.

Das hat verschiedene Vorteile.

- Die Geräte sind permanent dabei (Vor- und Nachbereitung, Sitzungen etc.).
- Jede Lehrperson kann die Peripherie eines Schulzimmers nutzen, ohne sich anmelden oder ein Profil wechseln zu müssen.
- Die Datenablage bleibt konsistent, es ist nicht mehr möglich, dass Daten aus Versehen auf dem festinstallierten Gerät gespeichert werden. Das erhöht auch die Sicherheit.

Bei der Ausrüstung der Lehrpersonen stellen sich mehrere Fragen:

Werden sämtliche Lehrpersonen ausgerüstet oder erst ab einem bestimmten Pensum?

Wir empfehlen aufgrund der deutlich gesunkenen Preise eine Ausstattung sämtlicher Lehrpersonen. Ansonsten müssten Poolgeräte oder weiterhin feste Arbeitsplätze zur Verfügung gestellt und aufwendig verwaltet werden.

Sind die Geräte persönlich?

Manche Schulen geben den Lehrpersonen keine Geräte mehr ab, sondern unterstützen den Kauf privater Geräte finanziell. Das ist für die Lehrpersonen flexibler, erhöht aber meist den Aufwand des Supportes (Betriebssysteme, Treiberproblematik bei Windowssystemen).

Sind die Geräte der Lehrpersonen gemanagt oder mit Admin-Rechten konfiguriert?

Wir empfehlen Adminrechte. Das ist deutlich flexibler, es gibt kaum mehr Gründe, die Geräte mit Nutzerprofilen auszustatten. Das gilt besonders, weil die Datenablagen weitgehend in der Cloud liegen.

Wie werden Geräteverwaltung und Backups gelöst?

Admin - Geräte bedeuten für die Lehrpersonen mehr Verantwortung, besonders bei der Datensicherung und Wiederherstellung. Es macht Sinn, sie dafür zu instruieren, und ihnen eine externe Festplatte abzugeben.

Der Support stellt eine Basisinstallation zur Verfügung.

Bei einer konsequenten Verwaltung und Administration der Geräte via Cloud ist selbst das nicht mehr notwendig, die Geräte können selbständig über das Internet neu aufgesetzt werden (zero touch*), die Verwaltung von Programmen und Einstellungen geschieht über eine Datenbank.

Wie gross sollen Laptops sein?

So gross wie nötig, so klein wie möglich. Grosse Laptops (16'') sind unhandlich und schwer, ersetzen aber trotzdem keinen Desktop mit grossem Bildschirm. Zudem sind grosse Laptops nicht mehr «state of the art», die Auswahl wird zunehmend kleiner.

Wie leistungsfähig müssen Geräte für Lehrpersonen sein?

Die Ansprüche an mobile Computer müssen durch reale Anforderungen und Bedürfnisse definiert werden und nicht durch Wünsche.
Die Beschaffung von teuren «Hochleistungsgeräten» macht keinen Sinn, aktuelle «Standard-Laptops» erfüllen oder übertreffen die Anforderungen.
Investieren sollte man in genügend Arbeitsspeicher und vernünftige Festplattengrössen, vor allem aber in Qualität und Langlebigkeit.

Auch Ansprüche an spezielle Technologien für KI-Anwendungen (NPU*) sind meist unnötig, sollten gut abgewogen sein und begründet werden können.

Gibt es Ausnahmen?

Beim Fachlehrerinnen- und Fachlehrersystem kann es sein, dass besondere Bedürfnisse vorhanden sind, etwa für Multimediaanwendungen (Bild- und Musikbearbeitungskurse). Das sollte im Einzelfall geprüft werden.

5.4.1 Schulverwaltung

Zur Schulverwaltung zählen das Schulpräsidium sowie sämtliche Verwaltungsangestellten. Hier sind heute zwei Ausstattungsvarianten üblich:

An den Arbeitsplätzen in der Verwaltung sind entweder Desktopcomputer installiert oder Laptops mit Dockingstationen.
Als Peripherie werden Maus, Tastatur sowie meist zwei externe Bildschirme genutzt. Je nach Bedarf kommt weitere Peripherie dazu (Scanner…).

Aus Sicherheitsgründen verfügen viele Schulen über eine lokale Datenablage, meist in Kombination mit einer cloudbasierten Datenplattform.

Die Arbeitsplätze der Schulverwaltung sind verwaltet und haben keine Admin-Rechte. Sie werden vollständig gesichert und durch den internen oder externen Support unterhalten.

Möglich ist, dass das Gerät des Schulpräsidiums adäquat zu den Geräten der Schulbehörde behandelt wird oder das Schulpräsidium neben dem Desktoparbeitsplatz noch einen mobilen Client nutzt (Laptop, Tablet…).

5.4.2 Schulleitung

Mitglieder der Schulleitung erhalten in jedem Fall ein Gerät der Schule gestellt. Üblicherweise sind das Laptops.

Die Arbeitsplatzausstattung ist adäquat der Verwaltung.

Die notwendige Software sowie der Zugang zum Netzwerk und der Datenplattform ist gewährleistet.

Falls Schulleitungen auf verschiedenen Datenablagen tätig sind, sollte gut abgewogen werden, wie intensiv der Datenaustausch ist und ob er uni- oder bidirektional* sein soll.

Das Handling einer solchen Lösung ist anspruchsvoll, damit einerseits die Übersicht nicht verloren geht, andererseits Daten nicht versehentlich auf die falsche Plattform gespeichert werden.

Setzt eine Schule vollständig auf eine Cloudumgebung, fällt diese Thematik weg. Durch ein geeignetes Rechtemanagement (policy) und entsprechende technische Vorkehrungen kann den unterschiedlichen Sicherheitsansprüchen Genüge getan werden.

5.4.3 Schulbehörde

Mitglieder der Schulbehörde erhalten nicht in jedem Fall ein Gerät der Schule gestellt. Wo das der Fall ist, sind es Laptops, allenfalls Tablets. Oftmals kommen BYOD-Ansätze zum Tragen. Dabei ist es relevant, dass die Daten sicher gehalten sind und auf dem privaten Gerät keine Schuldaten gehalten werden.

In solchen Fällen kann den Mitgliedern eine finanzielle Unterstützung geleistet werden, ebenso Unterstützung beim Support sowie notwendige Softwarelizenzen (Virenscanner…).

Die Geräte brauchen Zugang zur Datenablage der Schule (idealerweise cloudbasiert) sowie zu den schuleigenen Netzwerken.

Als Lifecycle bietet sich die Einsatzdauer einer Legislatur von vier Jahren an.

5.4.4 Mitarbeitende

Grundsätzlich handelt es sich um Schulgeräte ohne Adminrechte. Ob es Desktops, Laptops oder Tablets sind, hängt von den Ansprüchen ab. Einen Einfluss hat spezielle Software wie Schliesssystem, Technik- und Heizungsüberwachung etc.

Die Sicherheit und der Unterhalt liegen beim internen oder externen Support.

Ob Peripherie notwendig ist, hängt von der vorhandenen Basisinfrastruktur ab (Netzwerk, Druckerlösung, Backup).

Der Lifecycle ist adäquat der Geräte Schulverwaltung.

5.4.5 Gäste, Praktikanten und Praktikantinnen, Arbeitsgruppen

Das Zurverfügungstellen von Geräten wurde unter Punkt 5.2.6 beschrieben.

Der Zugang zum Schulnetzwerk wird bei diesen Nutzergruppen am besten über Voucher gelöst, für den Zugriff auf die Datenablage durch eine allgemeine Rolle mit entsprechenden Benutzerrechten.

Ähnlich wie Praktikantinnen und Praktikanten können auch Arbeitsgruppen gemanagt werden, bei denen interne Personen mit externen zusammenarbeiten. Das könnte zum Beispiel eine AG mit der Gemeinde sein, für ein Bauprojekt, ein Projekt mit anderen Schulträgern oder kantonalen Gremien etc.

5.5 Kauf, Miete oder Leasing

Sollen Geräte gekauft, geleast oder gemietet werden?
Diese Frage kann nicht allgemein beantwortet werden, jedes System hat Vor- und Nachteile.

- Der Kauf bietet die grösste Flexibilität bei der Einsatzdauer, dafür entstehen Kosten und Aufwand für Reparaturen oder Ersatz.
- Miete und Leasing bieten kalkulierbare Kosten inklusive Reparaturen und Ersatz, hingegen schliessen viele Leasing- oder Mietgeber kaum mehr Verträge über drei Jahre ab – diese Einsatzdauer ist wenig nachhaltig. Meist ist auch das Auskaufen nach Vertragsablauf unrentabel.
- Die Kosten beider Lösungen sind zwar vergleichbar, trotzdem liegen die Kosten für Miete oder Leasing höher. Kostentreiber sind die erwähnten Übernahmekosten nach Vertragsablauf.

Hinweis: Die unterschiedlichen Beschaffungsformen haben keinen Einfluss auf die Ausschreibungspflicht.
Die Schwellenwerte der verschiedenen Ausschreibungsverfahren setzen sich aus den Projektkosten über vier Jahre zusammen, also Kosten der Hardware sowie der geschätzten Supportkosten über dieselbe Laufzeit. Es spielt dabei keine Rolle, ob die Geräte gekauft, geleast oder gemietet werden.

5.6 Software

Wenn die Lehrergeräte mit Adminrechten versehen sind, können Lehrpersonen zusätzliche Software installieren. Das macht Sinn, einige Punkte müssen aber beachtet werden.

- Schulen müssen klar regeln, welche Software sie zur Verfügung stellt. Diese muss durch die Schule lizenziert werden.
- Lehrpersonen müssen darauf hingewiesen werden, dass sie private Software auf Schulgeräten selber lizenzieren müssen.
- Die Schule muss regeln, ob und welchen Support es für private Software gibt.

5.6.1 Virenschutz und Internetfilter

Geräte von Lehrpersonen müssen gegen Viren geschützt sein. Das Installieren und Aktualisieren eines Virenschutze sollte in der Verantwortung des Supports liegen.
Internetfilter (web content screening) machen auf Geräten von Lehrpersonen keinen Sinn, da sie etwa bei Recherchen einschränken (Googlesuche…). Zudem sind Lehrpersonen erwachsen und können selber beurteilen und verantworten, was sie im Internet nutzen.

6 Präsentationstechnik

6.1 Pädagogik

Wie in den meisten Infrastruktur-Bereichen gilt es auch hier, die pädagogischen Anforderungen zu klären Das gilt insbesondere für die Fragen, auf welche Art die Ausrüstung interaktiv genutzt werden soll.

Diese Interaktivität kann entweder direkt über das Display oder entsprechende Beamersysteme geschehen. Sie kann aber auch durch die Geräte der Nutzerinnen und Nutzer geschehen, besonders dort, wo «one2one»-Ausstattungen vorhanden sind.

6.2 Technik

Allgemein stellt man eine klare Verlagerung weg von Beamern hin zu interaktiven Displays (Touch-Systeme) fest.

Zudem haben sich die Datenübertragungen deutlich verbessert, die Bandbreiten haben sich vervielfacht, fehleranfällige Verbindungen wie HDMI werden durch HD-BaseT ersetzt.

6.3 Ökosystem

AV-Infrastruktur darf nicht nur für sich betrachtet werden. Eine Umgebung besteht aus der Vernetzung, der Energieversorgung sowie der Integration verschiedenster Eingabegeräte.

6.4 Im Detail

Unter folgendem Link finden sich detailliertere Informationen sowie Checklisten als Unterstützung bei der Entscheidungsfindung.

https://ict.vtgs.ch/angebote/praesentationsmedian-und-av-ausruestung

7 Drucker – Kopierer

Hinweis: Eine vollständige Zusammenstellung inklusive Checkliste für den Bereich Printing ist in Arbeit und wird hier verlinkt, sobald sie fertig ist (Stand Mai 2025).

Die Druckerausstattungen in den meisten Schulen ähneln sich stark.

Zentral gibt es leistungsfähige Grosskopierer, oft bestückt mit Sorter oder Finisher*.

Einzelplatz- oder Schulzimmerdrucker sind in einigen Schulen vorhanden, in anderen weitgehend verschwunden.

7.1.1 Einzelplatzdrucker

Es gibt zwei Arten von Einzelplatzdruckern:

- Einfache schwarzweiss-Laserdrucker in Schulzimmern. Sie sind gedacht, um «schnell etwas ausdrucken zu können».
  Bezogen auf die Lebensdauer, den Unterhalt und die Druckvolumina sind sie relativ teuer. Zwar benötigen sie lange keinen Toner, dann ist er aber meist teurer als der Drucker. Noch teurer wird es, wenn Fixiereinheiten ersetzt werden müssen.
- Einzelplatzdrucker als Laser-Farb-Multifunktionsgeräte, wo die Erreichbarkeit von zentralen Druckern schlecht gewährleistet, aufwendig ist oder besondere Anforderungen bestehen.
  Das können Drucker in externen Kindergärten, in der Schulverwaltung, bei der Schulleitung oder für den Hausdienst sein.

Kostenersparnis und Nachhaltigkeit können gefördert werden, wenn die Geräte mehrere Farbkartuschen haben, die einzeln ausgetauscht werden können. Diese Drucker sind in der Anschaffung teurer, im Unterhalt günstiger.

7.1.2 Grosskopierer

Sie stehen meist an zentralen Orten, beispielsweise dem Lehrerzimmer oder speziellen Arbeitsräumen für Lehrpersonen. Aus Vertraulichkeitsgründen stehen oft auch separate Systeme in der Schulverwaltung.

Die Geräte sind sehr leistungsfähig, neben hohen Druckgeschwindigkeiten überzeugen sie durch Finisher oder Sorter, etwa zum Druck von Broschüren.

Mit Benutzerauthentifizierung* können die Geräte auch an leicht zugänglichen Orten stehen, beispielsweise auf Schulhausgängen.

7.1.3 Anforderungen an die Drucksysteme

Je nach Anzahl der Nutzerinnen und Nutzer spielen die Geschwindigkeit sowie die Anzahl Papiermagazine eine Rolle. Es muss gewährleistet sein, dass die Drucker in den Spitzenzeiten fähig sind, die hohen Druckvolumina in nützlicher Zeit abzuarbeiten.

Spitzenzeiten sind der Morgen vor Schulbeginn, die Pausen, über Mittag und teilweise nach dem Unterricht.

Ebenfalls wichtig ist, dass möglichst viele verschiedene Medien bedruckt werden können.

Finisher zum Sortieren und Heften grösserer Druckaufträge sowie zum Erstellen von Broschüren sind bei solchen Geräten Standard, teilweise bereits intern oder als Anbaugeräte.

Insgesamt dürften die Ansprüche an diese Drucksysteme in den verschiedenen Schulen sehr ähnlich sein.

7.1.4 Druckkosten

Die Druckkosten setzen sich aus vier Grössen zusammen:

- Miete, Leasing oder Kauf der Geräte
- Klickpreise der gedruckten Seiten
- Anzahl der schwarzweissen oder farbigen Drucke
- Support und Unterhalt (Papier, Ersatzmaterial)

Die Druckvolumina sind in den Schulen sehr unterschiedlich, teilweise sehr hoch. Das ist auch nicht zwingend an die Grösse der Schule oder die Menge der Nutzenden gekoppelt.

Es ist unklar, welche Faktoren darauf Einfluss haben. Eine Rückmeldung von Anbietern ist; bei Systemen mit Benutzerauthentifikation sind die Druckmengen signifikant tiefer.

Ebenfalls ein Kostentreiber kann der Einsatz von Klassenzimmerdruckern sein (siehe 7.1.1).

Auch hier gilt, falls diese Geräte im Netzwerk verwaltet und überwacht werden, wird weniger gedruckt.

Was ebenfalls hilft; wenn Schulleitungen und/oder Schulbehörden die Nutzerinnen und Nutzer dafür sensibilisieren, dass nur notwendige Drucke ausgelöst werden.

7.1.5 Druckerverwaltung

Das Management von Druckern und Kopierern geschieht heute weitgehend cloudbasiert. So wird Ersatzmaterial automatisiert nachgeliefert, Gerätestörungen werden direkt vom System an den Support geleitet, selbst Druckaufträge von zuhause aus sind technisch möglich.

8 Gerätemanagement

8.1.1 Clientsysteme

Die Verwaltung und Administration von Geräten in der Schule hat sich in den letzten Jahren massiv verändert. Der grösste Unterschied; viele Managementsysteme sind heute cloudbasiert.

Das kann sowohl die Organisation von Updates oder Softwareverteilungen sein als auch das «disaster recovery», also das Neuaufsetzen abgestürzter Geräte.

Das klassische «imaging», also das Erstellen einer Basiskonfiguration, die auf alle Geräte kopiert wird, ist unflexibel, aufwändig und stellt hohe Anforderungen an die vorhandenen Netzwerke.

Bei bestimmten Geräten oder Betriebssystemen ist die cloudbasierte Verwaltung schon länger im Einsatz, Apple-Systeme (Mac OS und I OS) setzen schon lange auf diese Technologie.

Windows-Systeme haben insbesondere durch die AZURE-Systeme* von Microsoft (Autopilot) aufgeholt. Es gibt kaum mehr technische Gründe für ein Gerätemanagement über klassische, lokale Serverinfrastruktur.

Das neue Kultwort dafür ist «zero touch»*, also kein händisches Eingreifen mehr beim Aufsetzen oder Aktualisieren der Computer.

Bei mobilen Systemen, insbesondere den weit verbreiteten Tablets, ist der Einsatz von MDM-Software (mobile device management)* praktisch zwingend.

8.1.2 Nutzerverwaltung

Die klassischen Imaging-Technologien haben sich verändert oder sind verschwunden.

- Die profilbasierte Verwaltung verliert an Bedeutung, immer mehr Geräte sind personalisiert, fast überall haben Lehrpersonen persönliche Arbeitsgeräte. Damit müssen nicht mehr verschiedene Nutzerinnen und Nutzer auf einem Gerät gemanagt werden.
- Die Zugriffe auf die vorwiegend cloudbasierten Datenablagen geschehen direkt durch die einzelnen Nutzerinnen und Nutzer über ihre Zugangsdaten, nicht mehr über Geräte, die von mehreren Personen benutzt werden.
- Dasselbe gilt auch auf Ebene der Schülerinnen und Schüler. «one2one»-Ausstattungen nehmen zu, häufig ab der vierten oder fünften Klasse.
  Damit werden weniger Geräte «shared»*, also von mehreren Nutzenden geteilt. Häufig wird etwa im Zyklus I auf unkomplizierte Szenarien gesetzt. Im Kindergarten und der Unterstufe ist der Anfall von persönlichen Dokumenten überschaubar. Daten können direkt auf den Datenablagen oder dem Gerät geschehen. Die Geräte können einfach dafür konfiguriert werden.

Man darf nicht ausser Acht lassen, dass sich die Nutzungskompetenzen auch bei jüngeren Kindern verändert haben. Es können Dinge vorausgesetzt werden, die so vor einigen Jahren noch nicht möglich waren, etwa eine Authentifizierung mit Nutzername und Passwort.

9 Software

9.1 Schulverwaltung (SVS)

Das sind Softwareprodukte, welche die Daten Mitarbeitenden managt und von der Schulverwaltung und der Schulleitung genutzt werden.

9.2 «Notenverwaltung» und Kommunikation

Verschiedene Applikationen unterstützen die Verwaltung von Beurteilung / Noten, Lernberichten, Elterngesprächen und -kommunikation, Klasseneinteilungen sowie sonderpädagogischen Massnahmen. Am weitesten verbreitet sind die Datenverwaltung Lernsysteme (DVL) von PUPIL, ESCOLA oder CMI/LehrerOffice.

Diese Programme bieten auch sichere Kommunikationslösungen mit Eltern, etwa Krankmeldungen oder das Zurverfügungstellen von Dokumenten.
Sie ermöglichen auch eine Kommunikation unter den Lehrpersonen, mit Schulleitung und Schulbehörde.

Der Datenschutz ist so weit gewährleistet, als sich Nutzerinnen und Nutzer vernünftig und verantwortungsvoll verhalten. Leider werden immer noch unverantwortliche Parallelkanäle genutzt (z.B. WhatsApp). Grundsätzlich sind die meisten Chat Varianten heikel, nur dediziert von der Schul-DVL angebotene Dienste sind klar abgrenzbar zu betreiben.

Die technische Sicherheit ist so gut wie das verwendete System. Sie sollte nicht überschätzt werden in einer Zeit, in welcher auch Grosskonzerne oder staatliche Institutionen gehackt und erpresst werden.

9.3 Standardsoftware

Standardapplikationen wie Word, Excel, PowerPoint oder Keynote oder Photoshop werden auf fast allen Geräten eingesetzt, sie sind zunehmend hybrid, können lokal auf dem Gerät als auch im Browser genutzt werden.

9.4 Unterrichtssoftware

Lernprogramme variieren heute weniger als früher. Exotische «Lernprogrämmchen» gibt es kaum mehr, viele Lernprogramme und -systeme liegen heute ebenfalls in der Cloud (Französisch, Englisch, Mathematik, Deutsch…).

Ein Problem dabei ist die Authentifizierung. Es gibt zwar verschiedene Ansätze, von einem «single sign on» (sso*) sind wir aber immer noch weit entfernt.

9.5 Spezialapplikationen

Schulen setzen verschiedene Spezialprogramme ein, etwa Finanzsoftware wie Abacus oder Lösungen für Schliess- und Alarmierungssysteme und weitere.

10 Datenarchitektur

Aufgrund der weiten Verbreitung beziehen sich die folgenden Abschnitte besonders auf Microsoft 365. Kaum eine Schule setzt andere Softwareprodukte ein, immer weniger Schulen arbeiten auf lokalen Datenablagen.

Glücklicherweise ist auch die Sensibilisierung gegenüber Kommunikationsmitteln wie Whatsapp gestiegen, glücklicherweise zunehmend verboten.

10.1 Datenablage und Kollaboration

Schülerinnen und Schüler, Lehrpersonen, Schulverwaltung, Schulleitung und Schulbehörde arbeiten heute weitgehend mit der Plattform Microsoft 365.

Die grosse Verbreitung erklärt sich sowohl mit der Vielfalt der Werkzeuge, den Konditionen für die Schulen, der Skalierbarkeit, der Datenhaltung in der Schweiz und vertraglichen Regelungen auf Bundesebene.

10.2 Datenschutz

Die Anforderungen an den Datenschutz sind rechtlich durch Vereinbarungen zwischen der Schweiz und der EU sowie den USA geschützt, das hat eine Studie im Auftrag der Stadt Zürich gezeigt. (https://www.lauxlawyers.ch/wp-content/uploads/2022/07/Cloud-Gutachten-fuer-OIZ-Stadt-Zuerich.pdf).
auch eine geklärte Rechtslage verlangt einen verantwortungsbewussten Umgang mit Daten entlang der geltenden Vorgaben.

Der immer wieder beschworene, unkomplizierte Zugriff des amerikanischen Staates auf Rechenzentren amerikanischer Unternehmen relativiert sich und wäre aufgrund der Verträge mit der EU und der Schweiz als Missbrauch zu werten.

Selbst in den USA wurden staatliche Zugriffe auf Daten grosser Unternehmen (Microsoft, Google, Apple) von Gerichten wiederholt abgelehnt.

Das grösste Risiko in Bezug auf den Datenschutz sind nach wie vor die Nutzerinnen und Nutzer, wenn sie nicht wissen, welche Daten relevant sind und über welche Kanäle sie ausgetauscht werden dürfen.

10.3 Personendaten

Personendaten, insbesondere besonders schützenswerte Personendaten unterliegen erhöhten Sicherheitsanforderungen.
Dies sind Daten zu Schülerinnen und Schülern wie Gesundheitsdaten, Massnahmen, Beurteilungen, etc. oder zu Mitarbeitenden der Schule wie Bewerbungsunterlagen, Gesundheitsdaten, etc.
Die Schule muss sich bewusst sein, wo solche Daten gespeichert und durch wen die Daten bearbeitet werden können. Bei Unklarheiten kann hier eine externe Unterstützung hilfreich sein.

10.4 Zugriffsmanagement und Berechtigungsstruktur

Das ist ein zentraler Punkt. Moderne Datenablagen verfügen über alle notwendigen Möglichkeiten zur Authentifikation.

Zentral ist, dass Schulen eine durchdachte Struktur mit entsprechenden Rollen und Zugriffsberechtigungen entwickeln. Dabei muss darauf geachtet werden, dass möglichst wenige Rollen Administratorenrechte erhalten. Die Grafik zeigt einen Auszug aus einer Berechtigungsstruktur für eine SharePoint-Ablage.

Einstiegsseite	1. Ebene	2. Ebene	Bibliothek / Liste / Kalender	K = Kalender, B=Bibliothek, L=Liste, S=Seite	Globale Administratoren	Gr-Schulleitung		Gr-Lehrpersonen	Gr-Schulbus	Gr-Hausabwart		Gr-Schulsozialarbeit
Portal												
	Portal Schule XY				V	L		L	L	L		L
			Schulhandbuch	B	V	M		L	L	L		L
			Organisatorisches	B	V	M		L				L
			Austausch	B	V	M		M				M
			Protokolle	B	V	M		L		L		L
			Unterrichtsmaterial	B	V	M		M				
				B	V							
				B	V							
		Schulsozialarbeit			V							L
			Kinder	B	V							M
			Prävention	B	V							M
					V							
		Schulbus / Hauswart			V	L			L	L		
			Schulbus	B	V	M			M			
			Hauswart	B	V	M				M		
	Portal Leitung und Verwaltung				V	L						
			Austausch	B	V	M						
			Traktanden - Behördensitzung	B	V	M						
			Protokolle - Behördesitzung	B	V	M						
			GL Sitzung	B	V	M						
ee		**Schulleitung**			V	L						
			Dokumente	B	V	M						
				B	V	M						
					V							
					V							
		Schulbehörde			V							
			Allgemein	B	V							
			Präsidium	B	V							
			Finanzen	B	V							
			Liegenschaften	B	V							
			Pädagogik / Schulentwicklung	B	V							
			(Schülertransport)	B	V							
				B	V							
				B	V							
				B	V							

Abkürzungen		
V	Vollzugriff	
B	Bearbeiten	Können Bearbeiten und Bibliotheken hinzufügen
M	Mitwirken	Können Elemente bearbeiten / Hochladen (empfohlen)
L	Lesen	Können Elemente lesen

Die Umsetzung geschieht vorzugsweise mit einem professionellen, externen Partner, welcher den internen Support auch bei deren Administration unterstützt.

10.5 Datenverarbeitung und Verschlüsselung

Die Speicherung personenbezogener Daten unterliegt dem Datenschutzgesetz sowie einer sinnvollen Verschlüsselung.

Da sich die entsprechenden Technologien laufend verändern, verzichten wir hier auf eine Auflistung technischer Möglichkeiten.

11 Sicherheitsarchitektur

11.1 Benutzer-Authentifizierung

Zumeist geschieht der Zugriff auf schulische Datenablagen oder Verwaltungslösungen via Benutzername und Passwort, teilweise durch eine zusätzliche Authentifizierung via SMS.

Hier lohnt sich ein sogenannter «single sign on - sso», der die Zugangsdaten für verschiedene Ablagen vereinheitlicht. Dabei sollen die Prozesse geklärt werden und sich an der zentralen Benutzerverwaltung (active directory – ad) orientieren

Die Zweifaktorauthentifizierung (2FA)* für den Zugriff auf oft benutzte Ablagen oder Software trifft auf wenig Verständnis. Hier macht es Sinn zu prüfen, in welchen Fällen diese notwendig und sinnvoll ist.

11.2 Firewalls und Netzwerksicherheit

Der Schutz der Netzwerke durch Firewalls, Intrusion Detection Systeme IDS (Angriffserkennungssystem) und Anti-Virus-Software ist zentral, ob sie nun lokal oder cloudbasiert geschieht. Ein möglichst guter, aber auch adäquater Schutz ist heute zwingend.

Allerdings darf man auch nicht ausser Acht lassen, dass Schulen kein Sicherheitsniveau gewährleisten können, wie das in grossen Unternehmen oder auf kantonaler oder Bundesebene Standard ist.

11.3 web content screening

Zentral ist ebenfalls ein Internetfilter, in erster Linie für Schülerinnen und Schüler, grundsätzlich aber für praktisch alle Zugriffe vom Schulnetzwerk aus.

Dieser Filter muss die rechtlichen Vorgaben zu Rassismus, Gewalt und Pornografie standardmässig erfüllen, gleichzeitig aber so flexibel sein, dass er angepasst werden kann.

So macht es Sinn, diesen Filter temporär aussetzen zu können, um etwa Recherchen oder Unterrichtsprojekte zu gewissen Themen zu ermöglichen.

Das muss sensibel und verantwortungsvoll geschehen.

11.4 Datensicherheit und Backup

Eine genügende Sicherheit von Daten und regelmässige Backups der Schul- und Verwaltungsdaten sind zwingend. Auch hier braucht es aber eine Abwägung, welche Mittel eingesetzt werden.

Daten von Schulleitung, Schulverwaltung und Schulbehörde sowie Lehrpersonen haben eine andere Bedeutung als Arbeitsblätter oder Präsentationen von Schülerinnen und Schülern.

Grundsätzlich wird heute mit dem sogenannten «inkrementelle» Snapshot-Ansatz gearbeitet. Ein Snapshot erstellt nicht eine vollständige Kopie der Daten, sondern fängt das Bild eines bestimmten Moments ein und speichert dieses. Ein Snapshot ist also eine Momentaufnahme der auf einem Speicherserver gespeicherten Daten, die im Falle eines Systemausfalls zur Wiederherstellung genutzt werden kann.

Dieses Vorgehen verbraucht weniger Speicherplatz und dauert weniger lang. Solche Snapshots können in verschiedenen Intervallen gemacht werden, mindestens einmal täglich sollte die Regel sein.

So ist gewährleistet, dass im Falle eines Cyberangriffs oder eines Systemabsturzes eine schnelle Wiederherstellung möglich ist.

Das gilt unabhängig davon, ob die Daten auf lokaler Serverinfrastruktur oder in der Cloud liegen.

12 Support und Wartung

12.1 Technischer IT-Support

Sinnvoll für eine Schule ist die Bereitstellung eines Helpdesks* und/oder eines zuverlässig gepflegten Ticketingsystems*.

Die Aufgaben und Kompetenzen der unterschiedlichen Supportlevel müssen definiert und in Pflichtenheften abgebildet werden.

Es gilt klar abzugrenzen, was technischer Support ist und was pädagogische Unterstützung (siehe Pt. 12.2).

12.1.1 «first level support»

Als «first level support» bezeichnet man kleinere Störungen von Hard- und Software, welche idealerweise durch einen Neustart behoben werden können.

Der technische «first level support» kann gut intern gelöst werden, wobei die Interventions- und Bearbeitungszeiten definiert und tiefgehalten werden sollten (max. 10 bis 15 Minuten), damit die Ressourcen effektiv genutzt werden können.

Je nach Organisation und Kompetenz kann der grosse Teil solcher Störungen durch Lehrpersonen selber behoben werden. Dazu können FAQs (frequently asked questions – oft gestellte Fragen), Anleitungen oder Checklisten unterstützen.

12.1.2 «second level support»

Der «second level support» wird von den vielen kleinen und mittleren Schulen ausgelagert, weil sie die notwendigen Ressourcen lokal nicht zur Verfügung haben. Zudem handelt es sich hier um gravierendere Störungen, die ein gutes KnowHow voraussetzen.. Viele Probleme können mithilfe von Fernwartungslösungen oder Videocalls gelöst werden.

Falls eine Schule entsprechende Ressourcen zur Verfügung stellen kann, ist es möglich, den second level intern zu lösen.
Dabei muss darauf geachtet werden, dass eine Stellvertreterlösung besteht (evtl. mit ein externen Anbieter) und die Mitarbeitenden regelmässig weitergebildet werden.

12.1.3 «third level support»

Der «third level support» bezieht sich meistens auf den direkten Kontakt mit dem Hersteller, er sollte dringend ausgelagert werden. Das können etwa Netzwerk- oder Serverstörungen sein, der Ausfall ganzer Systeme, die betriebsbehindernd sind, Probleme mit Sicherheitskomponenten wie Firewalls oder gar Cyberangriffe.

Hierzu sollte ein kompetenter, flexibler und potenter Partner gesucht werden, der über die Zertifizierungen der Anbieter der eingesetzten Hard- und Software verfügt.

Für Lehrpersonen, Schulbehörde und Schulleitung sowie die Verwaltung wird ein Ticketsystem benötigt. Dieses wird idealerweise erst durch den internen Support bearbeitet und wenn nötig an den externen Supporter eskaliert.

12.1.4 SLA

Sogenannte «Service Level Agreements» regeln, welche Leistungen zu welchen Konditionen erfüllt werden müssen. Viele Anbieter haben hier Standardangebote.

Schulen sollten vor dem Abschluss solcher Verträge ihre Anforderungen kennen und als Inhalt der Vereinbarungen definieren.

12.1.5 Wartungspläne und Updates

Es sollte unterschieden werden zwischen proaktivem Support (Wartung), der in vielen Bereichen automatisiert abläuft (Netzwerküberwachung, Updates, Backups und deren Kontrolle…) und den Support nach Bedarf, also nur dann, wenn Störungen auftreten oder bestimmte Anpassungen notwendig sind.

Die Verlagerung des System- und Dokumentenmanagements in die Cloud führt üblicherweise zu etwas höheren Wartungskosten jedoch zu niedrigeren Supportkosten. So fallen bei intelligenten Lösungen die Updates der Standardinstallation weg, da diese laufend im Hintergrund aktualisiert wird.

Das trifft auch auf das Aufsetzen der Geräte zu. Bei sogenannten «zero touch»-Programmen werden alle Eckdaten in einer Datenbank gespeichert und nach Bedarf abgerufen. Fällt ein Gerät aus, erhält der Mitarbeiter ein Ersatzgerät, meldet sich am System ab und nach relativ kurzer Zeit ist sein Gerät wieder einsatzbereit – und sieht aus wie vorher.

Falls gerade Aktualisierungen und Updates noch lokal gemanagt werden, sollte darauf geachtet werden, dass nicht zu viel in zu kurzer Zeit verändert wird und besonders, dass Updates erst installiert werden, wenn sie eingehend auf ihre Funktionalität geprüft wurden.

Ein bis zweimal im Jahr Updates zu machen, reicht vollkommen, einzig Sicherheitspatches sollen zeitnah eingespielt werden.

Sehr wenig Aufwand bedeutet es, wenn man mit den reinen Web-Applikationen arbeite, weil dort laufend mit aktuellen Versionen gearbeitet wird.

12.2 Pädagogischer Support

Diese Unterstützung richtet sich an Lehrpersonen und/oder Schülerinnen und Schüler. iScouts oder PICTS beraten Lehrpersonen beim Einsatz digitaler Medien im Unterricht, evaluieren Trends, unterstützen bei Projekten und kümmern sich um Prozesse für die Auswahl neuer Werkzeuge, sowohl bei Hard- als auch bei Software.

Beschreibungen zu Funktionen und Aufgaben finden sich auf den Websites der Ausbildungsstätten, da diese Ausbildung auch dort stattfindet (PHTG, PHSG, PHZH…).

Besonders wichtig; der technische und der pädagogische Support sollten möglichst personell getrennt werden. Sonst besteht die Gefahr – das zeigen die Erfahrung und Rückmeldungen amtierender Personen – dass PICTS/iScouts von technischen Problemen zugedeckt werden und die pädagogische Unterstützung auf der Strecke bleibt.

12.3 Supportfeedback / Evaluation

Allzu oft arbeiten Supporterinnen und Supporter in einer eigenen Blase, kriegen die Nutzerbedürfnisse nur schlecht oder einseitig mit.

Dabei bewegen sie sich in einer vermeintlich starken Position, weil sie die grossen Knowhow-Träger sind. Zu oft entscheiden Verantwortungsträger und IT selbständig über Erneuerungen. Dabei gehen die Ansprüche und Erfahrungen der Nutzerinnen und Nutzer oft vergessen.

Zur Optimierung der Lösungen sollten regelmässig Evaluationen durchgeführt werden.

Solche Feedbackrunden können per schriftlicher Umfrage, im Rahmen der ordentlichen Konvente oder durch Sitzungen mit repräsentativen Abordnungen geschehen.
Wichtig ist dabei, dass keinen falschen Hoffnungen geweckt werden. Also fragen Sie bitte nur nach, wenn auch wirklich Veränderungen möglich sind oder deklarieren Sie die Umfragen als konsultativ.

Es ist sinnvoll, wenn «IT» ein fixes Traktandum in Konventen wird. So wird es zur Gewohnheit, die Inputs sind meist überschaubar und ja nach Bedarf kann schnell reagiert werden. Üblicherweise gibt es dann auch weniger «angestauten Ärger».

Vorsicht; Lehrpersonen sind meist keine «Techies», sie kennen aber ihre eigenen und die Bedürfnisse des Unterrichtes. Wenn Lehrpersonen in corpore unzufrieden sind, spielt das technische Knowhow keine Rolle mehr. Und, sie sind der wichtigste Teil der Kundschaft.

Was nicht vergessen gehen sollte – dieses Feedback ist durchaus in beide Richtungen zu verstehen. Also auch die IT, PICTS und TICTS oder iScouts sollen ihre Bedürfnisse mitteilen können. Das dürfen besonders auch Informationen über geplante Änderungen sein, Hinweise zur Nutzung bestimmte Hard- und Software oder Abläufe, welche den Support optimieren können.

Wichtig; es geht um Bedürfnisse, nicht um reine Wunschlisten.

12.4 Vertrags- und Lizenzmanagement

Jede Schule sollte eine Übersicht über die laufenden IT-Verträge, deren Lizenzmodelle und -kosten erstellen und seriös pflegen. Oft werden Lizenzen bezahlt, die günstiger zu haben wären oder gar nicht mehr im Einsatz sind.

Die vorhandenen Lizenzen sollten sauber dokumentiert und Zahlungs- sowie Kündigungsfristen im Auge behalten werden. Das gilt im Übrigen auch für Garantien.

Ebenfalls ist darauf zu achten, dass eingesetzte Produkte sauber und vollständig lizenziert sind. Nicht zu vergessen; auch Hardware benötigt teilweise Lizenzen (Firewalls…).

Die Lizenzverwaltung kann intern oder durch einen externen Dienstleister betreut werden.

12.5 Inventarisierung

Ein vollständiges und aktualisiertes Inventar ist zentral. So behält man den Überblick über Geräte und Programme, die eingesetzt werden. Dazu gehören auch Garantieleistungen.

Neben den reinen Arbeitsgeräten können das AV-Geräte der Schule sein, Peripheriegeräte (Making…), Ersatz- und Verbrauchsmaterial, Telefonsysteme etc.

Hier bietet sich das Lifecycle-Management an. Wie alt sind die Geräte, wann wurden sie repariert, wie lange gilt die Garantie, wie ist der Beschaffungs- und Erneuerungszyklus?

Das Inventar muss revisionstauglich und Teil eines Internen Kontrollsystems (IKS) sein.

13 Erweiterbarkeit und zukünftige Entwicklung

13.1 Skalierbare Infrastruktur

Damit Infrastruktur in vernünftigen Zyklen ersetzt werden kann, sollte sie bezogen auf steigende Ansprüche oder technische Anforderungen flexibel sein.

Je mehr Geräte das Internet nutzen, umso stärker werden beispielsweise WLAN oder Firewalls belastet.

Häufig sind auch Updates und Upgrades* eine Herausforderung, weil sie bei gewissen Geräten plötzlich nicht mehr eingespielt werden können (Firmware*…).

Teilweise kann das aufgefangen werden, indem man Geräte beschafft, die (noch) Leistungsreserven haben oder nicht zu einer Generation gehören, deren «end of life» bevorsteht oder deren Support vorhersehbar abläuft.

Oft kann das bedeuten, dass man eher teurere Geräte anschafft, weil es sich im Verlauf ihres Einsatzes stark relativieren kann. Wenn statt eines besseren Gerätes während der Laufzeit mehrere weniger gute Geräte ersetzt werden müssen, kommt das oft teurer zu stehen.

Solche Komponenten sind etwa Switches, Firewalls, WLAN-Aps, auch bei Clientgeräten lohnt es sich, auf «technische Nachhaltigkeit» zu achten.

13.2 Trend Scouting

Die Veränderungen in der IT Welt haben sich ein Stück weit verlangsamt, die Kadenz von System- und Softwareupdates beispielsweise ist niedriger als noch vor einigen Jahren.

Was bleibt, ist die Herausforderung für Schulen, «am Ball» zu bleiben. Einerseits ist das zeitintensiv, andererseits nicht Teil des schulischen Alltags.

Somit lohnt es sich, diese Aufgabe zumindest teilweise an den externen Dienstleister zu vergeben. Das kann zum Beispiel ein halbjährlicher oder jährlicher Workshop sein bei dem aktuelle und zukünftige Entwicklungen vorgestellt werden und man gemeinsam bespricht, ob und wann das für die Schule relevant werden könnte.

Der Entscheid, welchen Einfluss das auf den Unterricht, also die pädagogische Seite, hat, muss bei der Schule bleiben.
Hierfür gibt es in den meisten Kantonen Netzwerke und Angebote etwa von den Bildungsdirektionen/Erziehungsdepartementen oder den pädagogischen Hochschulen.

13.3 Umgang mit Updates und Upgrades

Software- und Betriebsystemupdates richten sich nicht nach Schulgepflogenheiten oder dem Schuljahreszyklus. So stellt sich regelmässig die Frage, wann und wie oft Updates eingespielt werden sollen.

Wichtige Grundvoraussetzung; sämtliche Updates werden getestet, bevor sie eingespielt werden

- Sicherheitsupdates sollten sofort, auf jedem Fall innerhalb weniger Tage eingespielt werden.

- «Normale» Updates, etwa des Betriebssystems oder von Lern- und Standardprogrammen sind meist nicht dringend, ein halbjährliches oder jährliches Einspielen genügt.

Manchmal führen Updates zur Frage von Neu- oder Ersatzbeschaffungen, weil die aktuellen Systeme nicht mehr mit der vorhandenen Hardware kompatibel sind.

Bevor neue Geräte gekauft werden, sollte aber überprüft werden, ob nicht mit dem bestehenden System weitergearbeitet werden kann.

In den meisten Fällen haben solche Updates nur Folgen für neue Geräte mit deren zusätzlichen (Hardware-) Möglichkeiten. Das kann sein, dass Sensoren verbessert wurden, die Kameras höher auflösen, neue System-Apps aufgenommen wurden oder die Prozessoren mehr Möglichkeiten bieten.

Ein Wechselgrund kann sein, wenn eine zentrale Software nicht mehr unterstützt wird. Allerdings lohnt sich hier die Abklärung, ob es eventuell eine Alternative dazu gibt.

In den allermeisten Fällen gilt der Grundsatz «never change a running system» bis zum nächsten, ordentlichen Ersatztermin.

14 Begriffsklärungen und weiterführende Links

Glossar mit Erklärungen

Kürzel	Erklärung
VTGS	Verband Thurgauer Schulgemeinden
CoC-ICT	Kompetenzzentrum für Informations- und Kommunikationstechnologien des VTGS
ICT | IKT	Information & Communication Technologies Informations- und Kommunikationstechnologien
IT	Information Technology | Informationstechnik oder Informatik
1. Zyklus	Nach Lehrplan 21, Kindergarten und 1.-2. Klasse
2. Zyklus	Nach Lehrplan 21, 3.-6. Klasse
3. Zyklus	Nach Lehrplan 21, 7.-9. Klasse
Netzwerk	Die Verbindung von digitalen Geräten innerhalb der Schule, entweder per WLAN, Ethernet oder Glasfaser (LWL)
Switch	Netzwerkverteiler
Rack	Ein abschliessbarer Schrank, in dem Firewall, USV, Switches und Server versorgt werden.
USV	Unterbrechungsfreie-Spannungs-Versorgung, eine Pufferbattierie für wichtige Bauteile, etwa Server und Firewall, die bei einem Stromausfall ein abruptes Ausschalten verhindern, sondern den Betrieb eine gewisse Zeit aufrechterhalten können oder ein kontrolliertes Herunterfahren der Systeme ermöglichen.
Firewall	Ein Gerät zur Kontrolle des Datenverkehrs vom Internet in die Schule und von der Schule ins Internet. Es funktioniert als Filter.
MBit/s, Gbit/s	Mass für die Datenrate, also dafür, welche Datenmenge über ein Netzwerk transportiert werden kann.
WLAN	«wireless area network» - Funknetzwerk, das aus mehreren Funkstationen (access points – Aps) besteht.
MIMO	https://de.wikipedia.org/wiki/MIMO_(Nachrichtentechnik)
WIFI 6	Standard für Funknetze
Routing	Das automatische Verbinden von Netzwerken, damit Nutzerinnen und Nutzer unterbruchsfrei «übergeben» werden – oft auch als «hand over» bezeichnet.
SSL/TLS	256-Bit Verschlüsselung wird in SSL/TLS-Protokollen verwendet, um sicherzustellen, dass die Datenübertragung zwischen Servern und Clients absolut sicher ist.

Kürzel	Erklärung
256 Bit	Eine 256-Bit-Menge kann 2^{256} verschiedene Werte speichern und ist eine der aktuell stärksten Verschlüsselungen. Theoretisch braucht es Milliarden von Jahren, um einen solchen Schlüssel zu knacken und würde die Energie Tausneder Kernkraftwerke benötigen.
direktional	Das bedeutet die Richtung, wie Daten übertragen werden. Wenn es nur in eine Richtung geht, heisst das «unidireaktional», in beide Richtungen «bidirektional».
Ethernet	Ethernetkabel gibt es in verschiedenen Kabelkategorien. Eine brauchbare Verkabelung benötigt mindestens Kategorie 5e, besser sind die Kategorien 6, 7 oder 8 (Stand 2025). Sie können bis zu 100 Meter lang sein und zwischen 100 Mbit/s bis 1000 Mbit/s verarbeiten. Für längere Distanzen müssen entweder Repeater oder Switches genutzt werden.
LWL	Alternativ zum Ethernet sind sogenannte Lichtwellenleiter (Glasfaser). Sie werden in sogenannte OM-Standards (Multimode) kategorisiert. Dabei wird bei OM1 und OM2 mit LED-Licht gearbeitet, bei OM3 bis OM5 wird Laserlicht genutzt. Mit OM3 bis OM5 können Distanzen von mehreren Kilometern mit 10 bis 100 GBit/s realisiert werden. Für noch weitere Verbindungen von mehreren hundert Kilometern gibt es Kabel der OS-Kategorien (Singlemode).
best effort	Theoretische Maximalleistung für Internetzugänge, welche verschiedenen Nutzergruppen offenstehen, also nicht exklusiv sind.
Mietleitung	Ein Internetzugang, der exklusiv für die mietende Kundin zur Verfügung steht (gemanagte Business Lösung). Sie zeichnen sich durch eine garantierte Bandbreite aus und sind meist in beide Richtungen (Upload und Download» gleich schnell. Dafür liegen die Kosten höher als bei «normalen» Internetzugängen und sie sind dem «Business-Bereich» vorbehalten.
IP Telefonie	Moderne Form der Telefonie, die nicht mehr über separate Telefonleitungen sondern über das Internet funktioniert. Diese Technologie wird heute auch in den meisten «Haustelefonen» verwandet. IP bedeutet Internet Protokoll und regelt, wie Daten über Netzwerke transportiert werden. Bei der Telefonie reden wir auch von VoIP (Voice Over IP), was die Übertragung von Sprache regelt.
Softclient	Ein Softwaretelefon, also ein Programm, das auf einem Rechner läuft und womit telefoniert werden kann.

Kürzel	Erklärung
Server	Oft versteht man darunter ein Gerät, das irgendwo im Keller oder in einem Rechenzentrum steht. Allerdings geht es nicht um das Gerät, sondern um die Software-Dienste, die darauf arbeiten. Das sind zum Beispiel Backup, Benutzerverwaltung, Geräteverwaltung, Netzwerküberwachung und weitere Dienste.
Virtuelle Server	Früher wurden Serverdienste auf mehrere Geräte verteilt. Heute werden die Dienste auf einem Gerät betrieben, die Software gaukelt dem System vor, dass es aus mehreren Geräten besteht (Instanzen). Virtualisierte Systeme sind genauso sicher, wie getrennte Rechner, ihre Verwaltung ist einfacher und effizienter.
NAS	«network attached storage» ist eine Netzwerkfestplatte, auf der ein minimales Serverbetriebssystem läuft, das einfache Serverdienste (Backup…) ermöglicht.
Redundanz	Das bedeutet, dass Systeme zweifach betrieben und synchronisiert werden, zum Beispiel zwei Server, die an verschiedenen Orten stehen. In Rechenzentren ist das der Standard.
VPN	Das ist ein «virtual private network», also ein Software-Tunnel, der meist als Zugriff auf Serversysteme gebraucht wird. Da der Tunnel vom Server aus geöffent wird, kann nur zugreifen, wer dazu eingeladen (authorisiert) ist. wenn dieser «Gast» seinen Zugang offenlässt, kann jedermann darauf zugreifen. VPNs werden heute nur noch von Profis benötigt uns sind nur so sicher, wie der Nutzer verantwortungsvoll damit imgeht.
«zero touch»	Das bedeutet, dass ein Computer nicht mehr langwierig aufgesetzt werden muss. Alle Informationen werden in einer Datenbank gespeichert, und wenn ein neues Gerät angeschlossen wird, passt die Datenbank alle Einstellungen und Programme automatisch an. Das neue Gerät ist in wenigen Minuten fertig konfiguriert und betriebsbereit. Das ist auch sehr praktisch, wenn ein bestehendes Gerät ersetzt werden muss. Ursprünglich wurde das Verfahren für Android-Systeme entwickelt.
Security, Policy	Das sind die Regeln für die Sicherheit eines Systems. Die Policy definiert, wer auf einem System oder einer Datenablage was tun darf, also ein Rechtemanagement. Ein Beispiel dafür sind die Ordnerberechtigungen auf einer Ablage wie SharePoint oder OneDrive.

Kürzel	Erklärung
Benutzerauthentifizierung	Wenn ich auf ein System oder eine Ablage zugreifen will, muss ich beweisen, wer ich bin – beispielsweise durch einen Benutzernamen und ein Passwort. Heute wird das oft mit einer Zweifaktorauthentifizierung gelöst. Zusätzlich zu den Zugangsdaten muss die Anfrage über einen Zugangscode via eine App oder über das Handy ergänzt werden.
sso	Als «single sign on» bezeichnen wir eine Lösung, die verschiedene Zugänge durch ein und dieselben Zugangsdaten automatisiert erlaubt. Zum Beispiel können dann die Anmeldedaten für den Computer auch für die Clouddatenablage oder bestimmte Online—Plattformen genutzt werden, ohne, dass man sich mehrmals anmelden muss.
Update	Unter diesem Begriff verstehen wir die Aktualisierung eines Software. Meist wird es durch die Anpassung der Nummern hinter der Softwareversion gekennzeichnet (Windows 10.5., Mac OS 14.4 etc.).. Wichtige Updates sind die sogenannten Sicherheitsupdates, sie sind dringender als «normale» Updates. Manchmal wird bei Updates auch von «patch» gesprochen.
Upgrade	Der Unterschied zu Update ist nur bedingt definiert. Meist reden wir von einem Upgrade, wenn die Versionsnummer sich ändert (Windows 10 zu Windows 11, Mac OS 14 zu Mac OS 15 etc.). Auf deutsch sprechen wir auch von einer Höherstufung oder Anhebung. Oft wird der Begriff Upgrade auch für eine Anpassung an der Hardware gebraucht (mehr Arbeitsspeicher, grössere Festplatte etc.).
Firmware	Als Firmware bezeichnet man sowohl die Betriebssoftware diverser Geräte oder Komponenten als auch die grundlegende Software eines Computers, die notwendig ist, um den Betriebssystemkern des eigentlichen Betriebssystems laden und betreiben zu können.
MDM	«mobile device management» meint ein Programm, um Tablets oder Smartphones zu verwalten.
Helpdesk	Die Ansprechsstelle für Support, das kann innerhalb der Schule sein, meist ist aber der Telefonsupport externer Dienstleister gemeint.
Ticketing	Bei einem Ticketsystem können Probleme online erfasst werden. Im Idealfall kann ich als Nutzerin oder Nutzer die Bearbeitung und Lösung meines Problemes mitverfolgen und mit dem Helpdesk auch kommunizieren, beispielsweise via Chat.

Kürzel	Erklärung
Convertible	Laptop mit Touchfunktion und der Möglichkeit, die Tastatur umzuklappen oder zu entfernen. Sie können also quasi als Tablet genutzt werden, sind 2 in 1 – Geräte.
NPU	Neural Processing Unit, ein spezialisierter Mikroprozessor, der die Leistung für Anwendungen für künstliche Intelligenz und maschinelles Lernen beschleunigt.
Sorter/Finisher	Zubehör zu Grosskopierern, damit man mehrseitige Dokumente sortieren, geheften oder als Broschüre drucken kann.

Weiterführende Links

Begriff	Weitere Informationen online
Videoüberwachung	https://www.datenschutz.ch/lexika/volksschule/videokameras
SSL / TLS	https://de.wikipedia.org/wiki/Transport_Layer_Security
256 Bit knacken	https://www.ssldragon.com/de/blog/knacken-ssl/
Mac-Adresse	https://de.wikipedia.org/wiki/MAC-Adresse
PUPIL	https://www.pupil.ch/
ESCOLA	https://escola.ch/
CMI Lehreroffice	https://cmi-bildung.ch/
Sicherheitskonzept Kanton Thurgau	https://av.tg.ch/themen/sicherheit-in-schulen.html/13464