SACHSEN-ANHALT

Leitlinien zur IT-Ausstattung an Schulen

Impressum

Herausgeber:

Ministerium für Bildung des Landes Sachsen-Anhalt

Turmschanzenstraße 32

39114 Magdeburg

http://www.mb.sachsen-anhalt.de

Magdeburg, September 2019

Inhaltsverzeichnis

Vorwort		6
1.	Einleitung	8
2.	Planung und Beschaffung von IT-Systemen in der Schule	10
2.1	Erstellung eines methodisch-didaktischen Medienbildungskonzeptes	11
2.2	Erstellung eines Medienentwicklungsplans des Schulträgers	11
2.3	Beschaffung von IT-Systemen	11
2.3.1	Grundsätze	13
2.3.2	Nutzungsdauer	14
2.4	Einsatz von Gebrauchtgeräten	15
2.5	Systembetreuung	15
2.6	Nutzungsordnung	18
2.7	Beratungs- und Fortbildungsangebote	19
3.	Infrastruktur-Komponenten und Netze	19
3.1	Schulinterne Netzwerkinfrastruktur	21
3.2	Internet-Zugang und –Bereitstellung	21
3.3	Internet-Gateway / Firewall-System	22
3.3.1	Kabelgebundenes Netzwerk (LAN)	22
3.3.2	Funknetze (WLAN)	24
3.3.3	Funkbrücken (Richtfunk)	25
3.3.4	Trennung der lokalen Netze in Teilnetze	26
3.4	Access-Points	26
3.5	Ethernet-Switche	26
4.	Ausstattung des digitalen Klassenzimmers	27
4.1	Arbeitsplatz-Komponenten	28
4.1.1	Arbeitsplatzrechner	28
4.1.2	Laptops	28
4.1.3	Tablets	29
4.1.4	Nutzereigene Geräte (BYOD)	29
4.1.5	Arbeitsplatz mit Präsentationseinrichtung	30
4.2	Lernplattform	31
5.	Weitere Einsatzbereiche von IT-Technik	33
5.1	Unterrichtsbezogene Nutzung von frei zugänglichen Computern	33
5.2	Lehrerzimmer	33
5.3	Ausstattung für die Seminarausbildung	34
5.4	IT-Systeme in der Schulverwaltung	34
6.	Software	35
6.1	Standardsoftware, Branchensoftware, pädagogische Software	35
6.2	Cloudbasierte Software	35
6.3	Lernprogramme	36
6.4	Betriebssysteme	36
6.4.1	Arbeitsplatzbetriebssysteme	36
6.4.2	Serverbetriebssysteme	36
6.4.3	Virtualisierung von Server-Systemen	37
7.	IT-Systemlösungen für Schulen	37

Anlage A Empfehlungen zum Umgang mit datenschutzrelevanten Daten an der Schule 38
Exemplarische Auflistung von datenschutzrelevanten Daten und Gerätezugriffen des Betriebssystems für den Einsatz im Klassenzimmer 40
Leitlinien zum Umgang mit dem Betriebssystem 41
Leitlinien zum Einsatz von Windows 10 im Klassenzimmer 42
Alternative Betriebssysteme 44
Leitlinien für Internetbrowser 45
Leitlinien für Suchmaschinen 46
Leitlinien für die Nutzung von Apps 47
Leitlinien für Büroanwendungen (Office) 48
Leitlinien für Internet-Gateway / Firewallsystem 49
Leitlinien für soziale Netzwerke, Chat, Messenger, Navigationsdienste 50
Leitlinien für die Passwortwahl 50
Leitlinien für E-Mail 51
Leitlinien für den Schulwebauftritt 52

Anlage B Hardware-Empfehlungen 55
Datenblatt Arbeitsplatzcomputer 55
Datenblatt Monitor 58
Datenblatt Notebook 60
Datenblatt Tablets 62
- Datenblatt PC-Tablet 62
- Datenblatt Android- bzw. ChromeOS-Tablet 64
- Datenblatt iOS-Tablet 66
Datenblatt Standardserver 67
Datenblatt Virtualisierung von Serversystemen 69
Datenblatt NAS-System für den Unterrichtsbetrieb 71
Datenblatt Einfaches NAS (z.B. zur Datensicherung) 75
Datenblatt Beamer 76
Datenblatt Großbildmonitor 78
Datenblatt Interaktiver Großbildmonitor (Touchscreen) 80
Datenblatt Dokumentenkamera 81
Datenblatt Drucker und 3D-Drucker 82
Strukturierte Gebäudeverkabelung 86
Datenblatt Access-Points 86
Datenblatt WLAN-Controller 89
Datenblatt Ethernet-Switche 91
Datenblatt Layer-3-Switche 93
Datenblatt Internetzugangsrouter 94

Glossar

Vorwort

Für den Einsatz digitaler Medien und Werkzeuge im Unterricht ist eine zeitgemäße digitale Mindestausstattung unabdingbar. Dazu gehören die Anbindung der Schulen an das Glasfasernetz, die Schulhausvernetzung einschließlich WLAN, der Zugang zu digitalen Lernplattformen, die Verfügbarkeit zeitgemäßer Präsentationstechnik und die Nutzung digitaler Endgeräte. Für die Internetanbindung der Schulen und eine jederzeit verfügbare und zuverlässige IT-Infrastruktur und IT-Ausstattung sind die Schulträger verantwortlich. Sie werden von Landesregierung und Bundesregierung unterstützt, u.a. durch den DigitalPakt Schule.

Im Sinne des Datenschutzes[1] und der IT-Sicherheit muss in den Schulen abgesichert sein, dass das Verwaltungsnetz vom pädagogischen Netz physisch getrennt ist. Die Vorgaben der Datenschutzgrundverordnung der Europäischen Union (EU-DSGVO) sind zu beachten.

Mittelfristig soll für alle Schülerinnen und Schüler das Arbeiten und Lernen mit digitalen Endgeräten und einer Lernplattform ermöglicht werden. Hinsichtlich der IT-Infrastruktur und IT-Ausstattung und aller damit zusammenhängenden Fragen empfiehlt sich eine enge Kooperation zwischen den Schulen und dem jeweiligen Schulträger.

Infrastruktur- und Ausstattungskonzepte sowie Medienentwicklungspläne der Schulträger für Schulen können nur auf der Grundlage von methodisch-didaktischen Medienbildungskonzepten der Schulen und im Einklang von pädagogischen und technischen Zielen entstehen. Auch die Ausstattung der Einrichtungen der Erwachsenenbildung soll schrittweise an moderne Standards angepasst werden.

Diese Leitlinien konkretisieren die zeitgemäße digitale Mindestausstattung, die für eine erfolgreiche pädagogische Nutzung an den Schulen notwendig ist. Es ist eine große Herausforderung, den Lehrenden und Lernenden an ihren Schulen angesichts des ständigen technischen Fortschritts im Hinblick auf Betriebssysteme, technische Ausstattung und Geschwindigkeit des Netzes möglichst vergleichbare Lern- und Zugangsmöglichkeiten bereitzustellen. Dies ist auch erforderlich, damit die Unterrichtsanforderungen möglichst an allen Schulen in vergleichbarer Form unterstützt werden können. Dazu dient vor allem eine standardisierte IT-Landschaft in der Schule. Dafür und mit Blick auf die Umsetzung des DigitalPakts Schule wurden die bestehenden Rahmenempfehlungen für die IT-Ausstattung von Schulen aus dem Jahre 2017 überarbeitet. Diese neuen Leitlinien, die künftig in regelmäßigen Abständen aktualisiert werden, geben eine Orientierung für die Ausstattung der Schulen mit Informations- und Kommunikationstechnik. Diese ermöglicht einen Unterricht, der den im Sinne der KMK-Strategie „Bildung in der digitalen Welt“ überarbeiteten Lehrplänen und den Vorgaben von Datensicherheit und Datenschutz gerecht wird.[2]

---

[1] Siehe die Ausführungen zu Security-by-Design, Privacy-by-Design/Default in der Einleitung und in Anhang A.

[2] Siehe Bildung in der digitalen Welt. Strategie der Kultusministerkonferenz, 2016, Download: https://www.kmk.org/fileadmin/Dateien/pdf/PresseUndAktuelles/2017/Strategie_neu_2017_datum_1.pdf, Abrufdatum: 03.09.2019 und Landeskonzept zur Umsetzung der KMK-Strategie „Bildung in der digitalen Welt“, 2018, Abrufdatum: 03.09.2019.

Gemeinsam schaffen Schulen und Schulträger die Voraussetzungen für modernes Lehren und Lernen in der digitalen Welt. Die Schulen können bei der Planung ihrer IT-Ausstattung am besten auf die Gegebenheiten vor Ort eingehen und passgenaue Lösungen finden.

Das ist auch die Orientierung der Digitalen Agenda für das Land Sachsen-Anhalt[3] und der Digitalen Jugendagenda.[4] Dabei stehen stets die Menschenwürde, die Unverletzlichkeit der Persönlichkeitsrechte und die digitale Souveränität eines jeden Einzelnen im Mittelpunkt.

Die angegebenen Maßnahmen sollen helfen, die Schülerinnen und Schüler, die Lehrkräfte und alle Interessierten in die Lage zu versetzen, den Mediengebrauch verantwortungsvoll und angemessen zu gestalten. Der Arbeitsgruppe aus unterschiedlichen Institutionen und allen, die die Erarbeitung mit ihren Hinweisen begleitet haben, danke ich herzlich für die geleistete Arbeit. Sie haben wichtige Impulse für die Konzeption und Umsetzung einer modernen IT-Ausstattung an den Schulen in Sachsen-Anhalt gegeben.

Hinweise und Anregungen zu den Leitlinien sind willkommen. Bitte richten Sie diese an MB-Referat16@sachsen-anhalt.de.

M. Tullner

Minister für Bildung des Landes Sachsen-Anhalt

[3] Digitale Agenda des Landes Sachsen-Anhalt, 2018, Download: https://digital.sachsen-anhalt.de/fileadmin/Bibliothek/Politik_und_Verwaltung/StK/Digital/DigitaleAgenda_Sachsen-Anhalt_Lesefassung.pdf, Abrufdatum: 03.09.2019.

[4] Jung und digital. Perspektiven und Forderungen junger Menschen zur digitalen Agenda des Landes Sachsen-Anhalt, 2018, Download: https://www.fjp-media.de/wp-content/uploads/sites/10/2018/10/Digitale_Jugendagenda_fjpmedia_web.pdf, Abrufdatum: 03.09.2019.

1. Einleitung

Bildung in der digitalen Welt

In ihrer Ende 2016 veröffentlichten Strategie zur „Bildung in der digitalen Welt“ formuliert die Kultusministerkonferenz (KMK) verbindliche Anforderungen, „über welche Kenntnisse, Kompetenzen und Fähigkeiten Schülerinnen und Schüler am Ende ihrer Pflichtschulzeit verfügen sollen, damit sie zu einem selbstständigen und mündigen Leben in einer digitalen Welt befähigt werden“.[5] Konkret wird dieses Ziel in sechs Kompetenzbereichen ausgedrückt:

- Suchen, Verarbeiten und Aufbewahren
- Kommunizieren und Kooperieren
- Produzieren und Präsentieren
- Schützen und sicher Agieren
- Problemlösen und Handeln
- Analysieren und Reflektieren.

Zeitgemäße Medienbildung ist ein System sich wechselseitig bedingender und unterstützender Komponenten. Dazu gehören vor allem

- das Landeskonzept zur Umsetzung der KMK-Strategie, das seit 2018 vorliegt[6]
- schulbezogene Medienbildungskonzepte
- die verbindliche Integration der Bildungsthemen zur digitalen Welt und des digital-vernetzten Lernens in alle Fachlehrpläne (ab 2019)
- verbindliche Angebote in allen Phasen der Lehrerbildung
- Verfügbarkeit geeigneter Medien, Materialien (Content) und Werkzeuge
  Beispiele sind die Materialien rund um das Internet-ABC, die Initiativen ‚Digitale Bildung trifft Schule‘ und ‚Bottom up – IT-Sicherheit für Berufsschüler‘ sowie der Einsatz des Minicomputers Calliope in unterschiedlichen Fächern und Projekten.[7]
- Test- und Nachweismöglichkeiten erworbener Medienkompetenzen (Medienbiber, Internet-ABC – Surfschein, Sachsen-Anhalt Medientest)
- koordinierte Netzwerke und Veranstaltungsformate zum digital-vernetzten Lernen (lokal, regional, Land)
- das Lernen mit digitalen Medien und Werkzeugen als Qualitätskriterium der Unterrichts- und Schulevaluation
- begleitende (Medien-)Bildungsforschung.

Ohne eine zeitgemäße digitale Mindestausstattung bliebe vieles im Ansatz stecken.

[5] Bildung in der digitalen Welt. Strategie der Kultusministerkonferenz, Berlin, 2016 (überarbeitet 2017), Download: www.bildung-lsa.de/medienberatung.html, Abrufdatum: 29.07.2019.
[6] Landeskonzept zur Umsetzung der KMK-Strategie „Bildung in der digitalen Welt“, 2018, Download: www.bildung-lsa.de/medienberatung.html, Abrufdatum: 29.07.2019.
[7] Siehe www.internet-abc.de, www.digibits.de, www.dsin-berufsschulen.de und www.calliope.cc (Abrufdatum jeweils: 31.08.2019).

Digitalisierung in Sachsen-Anhalts Schulen, aber sicher!

„Bei der Gestaltung der Digitalisierung müssen für uns stets die Menschenwürde, die Unverletzlichkeit der Persönlichkeitsrechte und die digitale Souveränität eines jeden Einzelnen im Mittelpunkt stehen.“[8] Grundprinzipien der Technikgestaltung sind:

- **Security-by-Design:** Bei der Entwicklung und Implementierung von Hard- wie Software wird bereits von Anfang an darauf geachtet, die Systeme so frei von Schwachstellen wie möglich und so unempfindlich gegen Angriffe wie möglich zu konzipieren. Denn mit dem laufenden Projektfortschritt steigen die Kosten für die Beseitigung von Sicherheitslücken.
- **Privacy-by-Design/Privacy-by-Default:** "Privacy" ist das englische Wort für Privatsphäre und Privatheit. Es wird auch mit Blick auf den Datenschutz verwendet. Datenschutz wird bereits bei der Konzipierung, Entwicklung und Implementierung von Software und Hardware zur Datenverarbeitung berücksichtigt. Durch benutzerfreundliche Voreinstellungen werden nur die Daten erhoben, die für den jeweiligen Verarbeitungszweck erforderlich sind, damit der Datenschutz sichergestellt und nicht bzw. möglichst wenig in die Schutzrechte der betroffenen Nutzer eingegriffen wird. Diese Einstellungen sind wegen des erhöhten Schutzbedarfs der Kinder im Sinne der UN-Menschenrechts-konvention und entsprechend Artikel 25 DSGVO zwingend notwendig.

Die in den Leitlinien formulierten Anforderungen und Handlungsbedarfe konkretisieren die Grundprinzipien der Technikgestaltung. Ziel ist es, die Planung, Konzeption, Umsetzung, Inbetriebnahme, den Betrieb und die Aussonderung von IT souverän und sicher zu gestalten sowie dem Verlust der Datensouveränität vorzubeugen. Entscheidend sind die Auswahl an Werkzeugen und deren geeignete Konfiguration (im Sinne einer digitalen Selbstverteidigung). Damit können im Bedarfsfall auch Nachbesserungen erzielt werden, die nicht nur als Anforderungen für die Planung und Realisierung hilfreich sind, sondern auch in der laufenden Anwendung der IT an Schulen dringend zu empfehlen sind. Dafür müssen die Verantwortlichen und Betroffenen befähigt und – ggf. durch Beratung und Fortbildung - in die Lage versetzt werden, den Geräte- und Mediengebrauch verantwortungsvoll und angemessen zu gestalten.

Die Inhalte sind exemplarisch ausgewählt, um allgemein den Handlungsbedarf sowie die Gestaltungsmöglichkeiten nach dem aktuellen Stand der Technik aufzuzeigen. Weitere Orientierungshilfen werden in der Datenschutzkonferenz und im BSI IT-Grundschutz gegeben.[9]

[8] Digitale Agenda für das Land Sachsen-Anhalt, Punkt 7 Querschnittsziele: Verbraucherschutz, Datenschutz und Informationssicherheit.

[9] Siehe https://www.datenschutzkonferenz-online.de/orientierungshilfen.html, https://www.datenschutzkonferenz-online.de/media/oh/20180426_oh_online_lernplattformen.pdf und https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html, Abrufdatum: 29.07.2019

2. Planung und Beschaffung von IT-Systemen in der Schule

In Vorbereitung von Beschaffungsmaßnahmen im IT-Bereich wird empfohlen, an der Schule eine Steuerungsgruppe einzurichten, die vor allem die Erarbeitung eines methodisch-didaktischen Medienbildungskonzeptes[10] und die Arbeit mit digitalen Medien und Werkzeugen an der Schule koordiniert. Die Steuerungsgruppe sollte aus Vertretern der Schulleitung und des Kollegiums bestehen und die technischen Anforderungen an den Medienentwicklungsplan des Schulträgers mit dem Sachaufwandsträger abstimmen. Kooperation und Konsens der Beteiligten sind wichtig, um Akzeptanz für nachhaltige Lösungen zu erzielen und eine tragfähige Entscheidungsgrundlage für die kommunalpolitischen Gremien zu schaffen. Insbesondere beim Auf- und Ausbau der standardisierten IT-Infrastruktur ist eine enge Abstimmung und Kommunikation mit dem jeweiligen Schulträger notwendig, um effiziente und nachhaltige Investitionsentscheidungen zu treffen, die den Anforderungen von IT-Sicherheit und Datenschutz genügen.[11] Unterstützung bietet die Landeskoordinierungsstelle für nachhaltige digitale Infrastrukturen für Unterricht und Schulen (LINDIUS)[12].

Die Steuerungsgruppe prüft die mittelfristigen Realisierungsmöglichkeiten und verfolgt die konkrete Umsetzung. Bei komplexen Planungen im Bereich der vernetzten Systeme ist es empfehlenswert, dass die Schulträger externe Experten[13] in die Planung einbeziehen und dies auch bei der Finanzplanung berücksichtigen.

Im Sinne von „Green IT“ ist schon bei der Planung auf einen dauerhaft ressourcenschonenden und damit nachhaltigen Einsatz der IKT zu achten.[14]

Bei der Außerdienststellung von IT-Technik ist insbesondere auf die sichere Löschung aller Datenträger zu achten.[15]

---

[10] Dies ist auch die Grundlage für das technisch-pädagogische Einsatzkonzept einer Schule, für die der Schulträger Fördermittel aus dem Digitalpakt beantragt (siehe 2.1). Das technisch-pädagogische Einsatzkonzept kann auch auf der Grundlage des Schulprogramms erstellt werden, wenn dort Medienbildung konkretisiert wird.

[11] Siehe die Ausführungen zu Security-by-Design, Privacy-by-Design/Default in der Einleitung und in Anhang A.

[12] Die Landeskoordinierungsstelle für nachhaltige digitale Infrastrukturen für Unterricht und Schulen (LINDIUS) wird im September 2019 am LISA eingerichtet.

[13] Gemeint sind z.B. die zuständigen medienpädagogischen Berater, IT-Fachberater, IT-Experten der Schulträger, IT-Experten der Ausbildungsbetriebe im beruflichen Umfeld, Ingenieurbüros, IT-Experten von Hochschulen.

[14] Siehe z.B. Korinna Sievert u.a.: Green IT. Arbeitsmaterialien für Schülerinnen und Schüler, hrsg. vom Umweltbundesamt, Dessau-Roßlau 2012, Download: https://www.umweltbundesamt.de/sites/default/files/medien/publikation/long/4258.pdf und educa.ch. Schweizer Medieninstitut für Bildung und Kultur: Green IT & Schule. Mit ICT Umwelt und Ressourcen schonen, o.D., Download: https://www.educa.ch/sites/default/files/greenit_de_1.pdf.

[15] Siehe dazu: Daten sicher löschen: Das müssen Sie beachten!, in: Datenschutz-Praxis, 23.04.2019, Download: https://www.datenschutz-praxis.de/fachnews/empfehlungen-tuev-daten-sicher-loeschen/, Abrufdatum: 03.09.2019.

2.1 Erstellung eines methodisch-didaktischen Medienbildungskonzeptes

Voraussetzung für Beschaffungsmaßnahmen im Kontext des DigitalPakts Schule[16] ist ein technisch-pädagogisches Einsatzkonzept. Dieses fasst das methodisch-didaktische Medienbildungskonzept der Schulen bzw. die Ausführungen zur Medienbildung im Schulprogramm zusammen[17] und bildet die Grundlage für die Medienentwicklungsplanung des Schulträgers. Das technisch-pädagogische Einsatzkonzept stellt die konkreten infrastrukturellen Komponenten und die mit der Förderung angestrebten Strukturverbesserungen im Sinne dieser Leitlinien ebenso dar, wie den Nutzen der technischen Veränderungen für die Umsetzung der angestrebten pädagogischen Ziele.

Beratung leisten die Landeskoordinierungsstelle für nachhaltige digitale Infrastrukturen für Unterricht und Schulen (LINDIUS) und die medienpädagogischen Beraterinnen und Berater des Landes. Ziel ist es, eine am realen Bedarf orientierte Medienentwicklungsplanung der Schulträger vorzunehmen, in regelmäßigen Abständen zu überprüfen und bei Bedarf fortzuschreiben.

2.2 Erstellung eines Medienentwicklungsplans des Schulträgers

Der Medienentwicklungsplan entsteht auf der Grundlage einer sorgfältigen Analyse der aktuellen Nutzung der Informations- und Kommunikationstechnologie und des Bedarfs der einzelnen Schulen. Dabei sollten folgende Punkte und Rahmenaspekte beleuchtet werden:

- Ist-Analyse: Aufnahme des technologischen Ist-Standes sowie der Kompetenz des Lehrerkollegiums[18],
- Ist-Analyse zu IT-Sicherheit auf Basis dieser Leitlinien bzw. aktuell geltender und absehbarer gesetzlicher Vorgaben (derzeit ISO 27001 auf der Basis von BSI IT-Grundschutz[19]; ggf. künftiges Audit/Gütesiegel) und zum Datenschutz mit dem zuständigen Datenschutzbeauftragten bzw. der Schulleitung,
- Integrations-Analyse: Möglichkeiten der Integration vorhandener Hardware bzw. Übernahme bereits in der Praxis erprobter und gefestigter Konzepte (Best Practice), z. B. aus dem Informatikunterricht,
- Bedarfsanalyse: Ergründung des Bedarfs anhand der entwickelten Medienbildungskonzepte / Medienentwicklungspläne,

[16] Siehe www.bildung-lsa.de/medienberatung.html, Abrufdatum: 31.07.2019.

[17] Für die Erarbeitung von Medienbildungskonzepten in den Schulen liegt eine Handreichung vor. Download: www.bildung-lsa.de/medienberatung.html.

[18] Siehe Anlage A in der Handreichung zur Erstellung von Medienbildungskonzepten: Vorschlag für einen Erhebungsbogen zum Qualifizierungsbedarf der Lehrkräfte.

[19] Siehe IT-Grundschutz-Kompendium: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html, Abrufdatum: 3.9.2019

- Matrix-Analyse: Vernetzung des Projektes mit laufenden bzw. zukünftig geplanten Projekten,
- Nachhaltigkeitsanalyse: Im Hinblick auf die technologischen Lösungen müssen Zukunfts- und Betriebssicherheit, Kosten-Nutzen-Verhältnisse, Wirtschaftlichkeitsbetrachtungen und Folgekosten betrachtet werden,
- Support-Analyse: Über einen entsprechenden Zeitraum muss mit dem IT-Partner / Lieferanten ein Support-Konzept sichergestellt werden. Bei der Nutzung von Rahmenvereinbarungen kann der Support auch zentral koordiniert werden. Hierbei sind insbesondere die Schulträger gefordert, ein ganzheitliches Konzept zu entwickeln, das den in diesen Leitlinien beschriebenen Anforderungen Rechnung trägt.

2.3 Beschaffung von IT-Systemen

Die Beschaffung von Hard- und Software sollte grundsätzlich in Abstimmung zwischen Schule und Schulträger erfolgen. Letztlich obliegt es dem Schulträger, über die Beschaffung zu entscheiden.

Beim IT-Einsatz stehen die didaktischen Aspekte und medienpädagogischen Ziele der jeweiligen Schule im Vordergrund. Grundlegende Standards für die Ausstattung der Schulen mit Informations- und Kommunikationstechnik bedingen die technischen Notwendigkeiten.

Neben den Empfehlungen und Festlegungen in diesen Leitlinien bedarf es bei einer konkreten Beschaffungsmaßnahme einer Ausschreibung gemäß den gesetzlichen Bestimmungen. Bestehende und ggf. neu zu schaffende Rahmenvereinbarungen bzw. Warenkörbe sind anhand der Maßgaben zur Beschaffung von IT-Systemen aus dieser Leitlinie zu prüfen und unter den erforderlichen Bedingungen neu auszuschreiben.

Bei der Anschaffung von neuer Hard- und Software muss ein besonderer Fokus auf die bereits vorhandene Infrastruktur und den Grad an verbindlicher Standardisierung gelegt werden. Diese muss skalierbar gestaltet sein, um so zusätzliche Möglichkeiten zu eröffnen, so dass

- Ressourcen besser genutzt werden und der Unterricht unter Einsatz von vorhandenen, aber auch neuer Lehrmittel erfolgen kann,
- neue Lehrmittel, periphere Geräte sowie Endgeräte der Lehrkräfte mit der bereits vorhandenen Ausstattung der Schule harmonisiert zusammenarbeiten können,
- durch Ergänzung der vorhandenen Infrastruktur ein neues Lehrpotenzial geschaffen und angewandt werden kann.

Im Rahmen der Akkumulation von Hardware- und Software-Komponenten ist auf offene Schnittstellen und einheitliche standardisierte technologische Komponenten zu achten, die den Supportaufwand explizit senken, da diese einheitlich und zentral administriert werden können. Aus Gründen der Nachhaltigkeit und der technischen Souveränität sind insbesondere offene Lösungen zu prüfen.

2.3.1 Grundsätze

Bei Neuanschaffungen sollte das IT-System komplett einschließlich einiger Ersatz-Computer und eines Grundbestandes der erforderlichen Software beschafft werden. Es ist sinnvoll, die zentrale IT-Technik - wie z.B. Switche, Controller, Firewall – in einem Technikraum zu installieren und die Unterrichtsräume jeweils vollständig mit kompatibler Hardware und Software auszustatten.

Bei Software-Beschaffungen zu einem späteren Zeitpunkt muss überprüft werden, ob die neue Software an den vorhandenen PCs eingesetzt werden kann oder höhere Hardware-Voraussetzungen erfordert. Ebenso muss bei Ersatzbeschaffungen von Hardware überprüft werden, ob die vorhandene Software am neuen System noch lauffähig ist und weiterverwendet werden kann.

Bei einer Beschaffungsmaßnahme darf nicht allein der Gerätepreis ausschlaggebend sein. Dienstleistungen wie Gewährleistung, qualifizierte Betreuung, Installation u. ä. oder auch entsprechende Administrationshilfen sollen in die Kaufentscheidung mit einbezogen werden. Des Weiteren sollte die Hardwarebeschaffung vor dem Hintergrund des Lebenszykluskostenkonzeptes unter wirtschaftlichen Gesichtspunkten bewertet werden.

Ein schulgeeignetes IT-System sollte unter Berücksichtigung des jeweiligen Einsatzbereichs folgende Mindestvoraussetzungen erfüllen:

- Die Gewährleistung durch den Fachhändler oder einen Drittanbieter sollte bei sämtlichen Baugruppen für einen Zeitraum von mindestens 36 Monaten gegeben sein (Vor-Ort-Service während der Gewährleistungsfrist, ansonsten Bring-In-Service).
- Wird die Nutzung professioneller Gebrauchtcomputer angestrebt (gilt nicht für geförderte Investitionen), so müssen abweichende aber hinreichende Gewährleistungszeiträume vereinbart werden.
- Mithilfe eines Service-Level-Agreements (SLA) können Leistungsumfang, Reaktionszeit und Schnelligkeit der Bearbeitung genau beschrieben werden. Wichtiger Bestandteil ist hierbei das Servicelevel, welches die vereinbarte Leistungsqualität beschreibt und Angaben zum Leistungsspektrum (z. B. Vor-Ort-Austausch von Geräten), zur Verfügbarkeit und zur Reaktionszeit des Anbieters enthält.
- Beim Austausch defekter Computer sollte darauf geachtet werden, dass die Hardware die Installation verschiedener Betriebssysteme ermöglicht.
- Der betreuende Fachhändler muss über genügend Fachkompetenz in Bezug auf Schulausstattungen verfügen. Eine vollständige Installation, ein formelles Abnahmeprotokoll sowie ein längerfristig verfügbarer technischer Vor-Ort-Support mit einer angemessenen kurzen Reaktionszeit müssen gewährleistet sein.
- Die Bauweise der einzelnen Komponenten soll instandhaltungsfreundlich sein, geringe Störanfälligkeit und niedrige Reparaturkosten gewährleisten.

- Sehr wichtig ist auch die Einhaltung ergonomischer Anforderungen entsprechend der Arbeitsstättenverordnung[20] und die Beachtung von Umweltrichtlinien und Barrierefreiheit.

  Hervorzuheben sind:

  - Geräuschentwicklung
  - Tastatur mit geneigtem und leicht bedienbarem Tastaturfeld mit leisem Anschlag, geeignet zum Tastschreiben
  - Bildschirm mit matter Oberfläche, Höhe und Neigung verstellbar
  - Drucker mit geringer Feinstaubemission, insb. bei hohem Druckaufkommen
  - Umweltprüfzeichen Energy Star als Zertifikat für energieeffiziente Geräte (z.B. Energy Star 6.1 für Computer und Monitore)
  - TCO-Zertifikate (TCO Certified Displays 7 für Monitore, TCO Certified Notebooks 5, TCO Certified Tablets 3, TCO Certified Projectors 8 für Beamer)
  - „80 Plus"-Zertifizierung von Netzteilen, um einen möglichst hohen Wirkungsgrad in den verschiedenen Lastbereichen zu gewährleisten
  - Umweltprüfzeichen Blauer Engel (z. B. RAL-UZ 78a für PCs, RAL-UZ 78c für Monitore, RAL-UZ 171 für Drucker)
  - GS-Prüfzeichen und Funkentstörung nach CE-Norm (auch für Einzelteile!)
  - umweltfreundliches Material von Verpackungen – mit Rücknahme und fachgerechter Entsorgung durch den Anbieter
  - Rücknahme von Altgeräten durch den Lieferanten entsprechend den gesetzlichen Bestimmungen.

2.3.2 Nutzungsdauer

IT-Geräte und -Komponenten sollten so beschafft werden, dass eine wirtschaftlich sinnvolle Nutzungsdauer möglich ist. Nach derzeitigen Praxiserfahrungen beträgt die Nutzungsdauer für mobile Endgeräte ca. fünf Jahre, für Arbeitsplatzcomputer bis zu sieben Jahre. Bei Servern, die für den Betrieb unverzichtbar sind, ist die Nutzungsdauer üblicherweise an die Dauer der Garantieleistung durch den Hersteller (in der Regel fünf Jahre Vor-Ort-Garantie) gekoppelt.

Bei den aktiven Netzwerkkomponenten (z. B. Router, Switche, Access-Points) kann von einer Lebensdauer von zehn Jahren ausgegangen werden, wobei Internetzugangsrouter in der Regel bei einer Änderung des Internetzugangs getauscht werden müssen. Auch bei Access-Points ist ein früherer Austausch dann sinnvoll, wenn insgesamt auf eine aktuelle WLAN-Technologie umgestellt werden soll – falls die Notwendigkeit dazu begründet vorliegt.

[20] Siehe Arbeitsstättenverordnung, 6. Maßnahmen zur Gestaltung von Bildschirmarbeitsplätzen, https://www.gesetze-im-internet.de/arbst_ttv_2004/BJNR217910004.html, Abrufdatum: 30.07.2019.

Bei passiven Netzwerkkomponenten (Verkabelung, Patchfelder) kann von einer Nutzungsdauer von 20 Jahren ausgegangen werden, so dass dieser Bereich besonders sorgfältig geplant werden sollte.

2.4 Einsatz von Gebrauchtgeräten

Die Nachnutzung gebrauchter Hardware (gilt nicht für geförderte Investitionen) kann unter bestimmen Gesichtspunkten wirtschaftlich sein. Gebrauchte Geräte sind für den Betrieb in der Schule und insbesondere unter Verwendung ressourcenschonender, freier und Open Source Software oft noch leistungsfähig genug. Eine Annahme von Spendengeräten ist vor allem unter wirtschaftlichen Gesichtspunkten zu prüfen, maßgebend ist hier, dass die notwendige Wartung hinzugekauft und damit sichergestellt werden kann.

Wird die Nutzung professioneller Gebrauchtcomputer angestrebt (gilt nicht für geförderte Investitionen, hier Lebensdauer und Bindefrist beachten!), so müssen hinreichende Gewährleistungszeiträume im Rahmen der Bindefrist vereinbart werden. Mit der Bewilligung von Fördermitteln wird eine Bindefrist festgelegt.

Daher müssen die geförderten Wirtschaftsgüter fünf Jahre nach Anschaffung in der Schule verbleiben (= Bindefrist). Dieser Anspruch leitet sich daraus ab, dass die Bund-Länder-Vereinbarung die dauerhafte Schaffung von Infrastruktur und digitalen Lernumgebungen zum Ziel hat. Als „dauerhafte Schaffung von Infrastruktur und digitaler Lernumgebungen“ in diesem Zusammenhang gilt ein Wirtschaftsgut, das mindestens fünf Jahre lang in gleicher oder modernisierter Form dauerhaft auf dem Markt angeboten wird.

2.5 Systembetreuung

Die Betriebssicherheit der IT-Technik in Schulen ist notwendige Voraussetzung für die Umsetzung des Medienentwicklungsplans des Schulträgers und fällt in die Zuständigkeit des Schulträgers. Er muss dafür personelle Vorsorge treffen und geeignete räumliche Voraussetzungen schaffen. Für die externe Unterstützung bei der Systembetreuung empfiehlt sich der Abschluss von Service- und Wartungsverträgen, inkl. Softwareupdate und –upgrade.

Es empfiehlt sich, dass die Schulen für den First-Level-Support einen oder mehrere Personen benennen, die entsprechend zu schulen sind und in die Medienentwicklungsplanung des Schulträgers einbezogen werden können.

Es ist im Interesse der Lehrkräfte, bei Wartungs- und Pflegearbeiten ihre pädagogische Sicht – im Sinne eines „pädagogischen Lastenheftes“ - einzubringen. Das betrifft im Einzelnen:

- Mitwirkung bei der Planung und dem Ausbau von Netzstrukturen für unterrichtliche Anwendungen
- Einbeziehung in Planungen von unterrichtlich zu nutzenden Verzeichnisstrukturen, Zugangsberechtigungen

- Rechts- und Sicherheitsfragen bei der Internet-Nutzung, insb. auch Handhabung der Benutzerverwaltung und eines sicheren Konfigurationsschutzes
- Mitwirkung bei der Auswahl und Lizenzierung von Software
- Planung und Handhabung eines sicheren Konfigurationsschutzes und Benutzerverwaltung.

Aus praktischen Überlegungen heraus verbleibt die Unterstützung bei Anwendungsproblemen mit Software und dem lokalen Netzwerk in der Schule. Vor Ort sollte es Pädagogen geben, die bei Fehlbedienungen helfen und das Kollegium in der Handhabung von Software und Nutzung lokaler Vernetzung unterstützen und schulen können. Bei Defekten der Hardware und Problemen mit komplexen Konfigurationen, deren Behebung zeitaufwendig ist und entsprechendes Fachwissen und Erfahrung verlangt, ist auf Unterstützung des Second-Level-Supportes zurückzugreifen, für den der Schulträger Vorsorge trifft. Bei Beschaffungs- und Einrichtungsvorhaben sollte bedacht werden, dass auch die für den Betrieb notwendigen Kenntnisse vorhanden sein oder durch Schulungen vermittelt werden müssen.

Aufgaben der Schule

Die aus dem Kollegium mit dem First-Level-Support betrauten Personen übernehmen in der Schule die folgenden Aufgaben:

- Mitwirkung bei der Medienkonzeptentwicklung
- Unterstützung der Kommunikation zwischen den Schulgremien
- Information und Beratung zu Ausstattungsszenarien unter pädagogischen Gesichtspunkten
- Schnittstelle zur Steuerungsgruppe zwecks weiterer Informationsbeschaffung
- Schulung und Beratung des Kollegiums und ggf. des nicht-lehrenden Personals
- technischer Umgang und Benutzung der Multimediaeinrichtungen und des Netzwerks
- Schärfung des Rechts- und Sicherheitsbewusstseins – insb. hinsichtlich Datensicherheit und Datenschutz
- Ressourcenverwaltung
- Hilfe bei der Pflege der Inventarliste der Hard- und Software
- automatisierte Wiederherstellung von Arbeitsplätzen
- Behebung einfacher Fehler
- strukturierte Fehlermeldung an den Second-Level-Support
- Pädagogische Benutzerkontrolle
- Beteiligung an der Erstellung einer Benutzervereinbarung
- Unterstützung bei der Reglementierung von Fehlverhalten

Second-Level-Support

Die Aufgabe des Schulträgers ist der Aufbau des Second-Level-Supports als Teil der Medienentwicklungsplanung. Diese kann intern, aber auch durch den Einsatz externer Dienstleister sichergestellt werden.

Aufgaben im Rahmen des Systemmanagements

Ähnlich dem First-Level-Support gibt es regelmäßig wiederkehrende Wartungs- und Pflegeaufgaben, die aus Praktikabilitätsgründen zentralisiert und vom Second-Level-Support übernommen werden sollten.

Um einen ausreichenden Schutz zu gewährleisten, ist insbesondere bei der Firewall und bei den Filtern ein ständiger Aktualisierungsprozess der benötigten Daten erforderlich. An dieser Stelle sollten bei der technischen Bereitstellung des Schutzes zentrale Lösungen bevorzugt werden. Aktualisierungen der Software und der benötigten Daten müssen dann für alle beteiligten Schulen nur einmal durchgeführt werden.

Elemente des Second-Level-Supports

Zur Unterstützung des First-Level-Supports werden auf kommunaler Seite die folgenden Supportwerkzeuge als beispielhafte Möglichkeiten genannt. Die Hotline nimmt telefonische Störmeldungen vom First-Level-Support entgegen. Einfache Probleme können im Gespräch mit dem First-Level-Support gelöst werden. Ist dies nicht möglich, so wird ein Vor-Ort-Service notwendig. Das Personal muss über entsprechendes technisches Fachwissen verfügen. Die Kenntnis der EDV-Infrastruktur der einzelnen Schule ist zwingend erforderlich. Beantwortete Supportanfragen könnten in einer FAQ-Liste dokumentiert und online zur Verfügung gestellt werden und so die qualifizierte Dokumentation ergänzen.

Vor-Ort-Service

Störungen, die weder durch eine FAQ-Liste noch mit Hilfe der Hotline behoben werden können, beispielsweise komplette Neukonfigurationen oder Installation von Hardwareelementen, können nur durch fachkundige Techniker eines Vor-Ort-Services bearbeitet werden . Hierbei sind unterschiedliche Organisationsmodelle denkbar, kommunal getragene, rein privatwirtschaftliche und Mischformen.

Damit der laufende Unterricht mit der IT-Infrastruktur aufrechterhalten werden kann, sollte der zeitliche Abstand zwischen Supportanfrage und Behebung durch einen Techniker definiert sein (Service-Level-Agreements). Es empfiehlt sich, dies bereits bei der Beschaffung und in Wartungsverträgen zu vereinbaren.

Die Kommune oder von ihr beauftragte Dienstleister übernehmen folgende Aufgaben:

- Netzwerkgestaltung
- Aufstellung und Einrichtung der Geräte
- Verkabelung der Geräte/Räume
- Konfiguration des Netzwerkes
- Für die Reparatur defekter Geräte sorgen
- Behebung von Fehlfunktion des Netzwerkes
- Behandlung von Sicherheitsvorfällen
- Ressourcenverwaltung
- Inventarisierung der Hard- und Software
- Datei- und Benutzerstruktur definieren und ggf. einrichten

- Software nach Warenkorb im Netzwerk installieren
- Bereitstellung von Werkzeugen zur Benutzerpflege
- Entwurf und Überwachung eines Sicherungskonzeptes
- Schutz der Arbeitsplätze durch geeignete Sicherungsverfahren
- Wiederherstellung des Servers
- Virenschutz und Firewall installieren und aktualisieren
- Webmanagement
- Einrichtung des Internetzugangs
- Installation und ggf. Aktualisierung von Protokollierungs- und Filtersoftware

2.6 Nutzungsordnung

Bereits aufgrund geltender gesetzlicher Bestimmungen wie etwa der EU-DSGVO ist es grundsätzlich erforderlich, mit den Schülerinnen und Schülern sowie den Lehrkräften und dem Verwaltungspersonal eine Nutzungsordnung zum Umgang mit den IT-Systemen zu erarbeiten.[21] Sie sollte durch Beschluss der Gesamtkonferenz von allen schulischen Akteuren mitgetragen und ihre Kenntnisnahme durch Unterschrift (bei unter 14-Jährigen auch durch Unterschrift der Sorgeberechtigten) bestätigt werden.

Sollen schulische mobile Endgeräte im häuslichen Umfeld nutzbar gemacht werden können, muss dieses in der Nutzungsordnung geregelt werden. Werden private Endgeräte im schulischen Kontext genutzt (BYOD), ist dies ebenfalls in einer Nutzungsvereinbarung zu regeln. Die dort vereinbarten Regeln sollten prinzipiell unabhängig vom benutzten Endgerät sein.

Es empfiehlt sich, bei schuleigenen mobilen Geräten Regelungen[22] vor allem zu folgenden Themen zu treffen:

- Austeilen, Einsammeln, Aufbewahren und Laden der Geräte
- Möglichkeit zum Zurücksetzen, Klonen oder zur Neuinstallation der Geräte (Mobile-Device-Management, MDM).
- Datenschutz und Datensicherheit insbesondere in Bezug auf den Umgang mit personenbezogenen Daten (Verhaltensregeln, Sicherung der Ergebnisse, Löschen der Dateien vor der Aushändigung des Tablets an einen anderen Benutzer) und mögliche Urheberrechtsverletzungen im Umgang mit dem Internet (Upload bzw. Download von Dateien).[23]
- Support, Haftung.

[21] Ein Beispiel für eine Nutzungsordnung finden Sie in Anlage A.

[22] Ein Beispiel, wie man den Einsatz von BYOD regeln kann: https://www.msindersdorf.de/wp-content/uploads/2017/12/Nutzungsordnung_BYOD_2017_18_Endfassung.pdf. Siehe ferner Philippe Wampfler: 15 Grundsätze zu BYOD am Gymnasium, Download: https://schulesocialmedia.com/2017/04/04/15-grundsaetze-zu-byod-am-gymnasium/, Abrufdatum: 31.07.2019.

[23] Siehe die Ausführungen zu Security-by-Design, Privacy-by-Design/Default in der Einleitung und in Anhang A.

2.7 Beratungs- und Fortbildungsangebote

Die Schulung der Lehrkräfte und Administratoren bildet die Grundlage für einen erfolgreichen Einsatz der Technik an den Schulen. Beratung und Fortbildung rund um die Themen der IKT-Ausstattung von Schulen bietet das LISA mit

- der Landeskoordinierungsstelle für nachhaltige digitale Infrastrukturen für Unterricht und Schulen (LINDIUS)
- den Angeboten zur digitalen Bildung auf dem Bildungsserver des Landes[24]
- dem Einsatz der medienpädagogischen Beraterinnen und Berater des Landes.

Die bestehenden Beratungs- und Fortbildungsangebote zum Thema IT-Ausstattung von Schulen werden sukzessive ausgebaut und Schulträgern zugänglich sein. Nur so kann eine enge Kooperation und Koordination zwischen den Verantwortlichen, die auf ein Verständnis von Technik und deren pädagogisch-didaktischen Einsatz abzielt, gewährleistet werden.

Um eine erfolgreiche Umsetzung dieser Leitlinien im Zuge des Digitalpakts mit dem erforderlichen Umdenken in pädagogisch-didaktischer Sicht in Einklang zu bringen, ist die Beratung und Fortbildung ein zentrales Thema auf allen Ebenen. Einen besonderen Schwerpunkt bildet aktuell das ESF-Projekt zur Steuerung von Prozessen digital-vernetzten Lernens,[25] das den Fokus auf die Schulleitungen legt, die als Schnittstelle der Schulkoordination entscheidenden Einfluss bei der Motivation des Kollegiums und der Ermöglichung von notwendigen Veränderungen haben.

Zusätzlich bedarf es Multiplikatoren, die Konzepte zum Lehren und Lernen mit digitalen Medien und Werkzeugen in die Kollegien tragen und gemeinsam mit den medienpädagogischen Beraterinnen und Beratern Fortbildungen und Beratung zur Bildung unter den Bedingungen der digitalen Transformation anbieten. Darauf zielt auch das o.g. ESF-Projekt. Damit wären sie ständige Ansprechpartner für ihre Kollegien und darüber hinaus, können sie so ein funktionierendes Informationsnetzwerk, unterstützt vom LISA, aufbauen.

3. Infrastruktur-Komponenten und Netze

Mit dem Auf- und Ausbau der IT-Infrastruktur werden zentrale Voraussetzungen für eine nachhaltige Entwicklung bei der Digitalisierung der Schulen geschaffen. Am Anfang wird zuerst der Schwerpunkt auf das Gesamtbild gelegt, um ein Verständnis für die übergeordneten Zusammenhänge zu erzeugen und Verantwortlichkeiten besser verteilen zu können

[24] www.bildung-lsa.de/medienberatung.html (->Digitale Bildung).

[25] Das ESF-Projekt „Steuerung von Prozessen digital vernetzten Lernens – Programm zur Fortbildung und Qualifizierung von Mitgliedern der Schulleitungen in Sachsen-Anhalt“ richtet sich an schulische Führungskräfte in Sachsen-Anhalt, die sich in ihren Kompetenzen zur Steuerung von Prozessen digital vernetzten Lehrens und Lernens an ihren Schulen fortbilden wollen. Das Programm ist auf drei Jahre angelegt und endet am 31.07.2022. Ansprechpartner und weiterführende Informationen: https://landesschulamt.sachsen-anhalt.de/behoerde/fuehrungskraefteentwicklung/esf-projekt-steuerung-von-prozessen-digital-vernetzten-lernens-programm-zur-fortbildung-und-qualifizierung-von-mitgliedern-der-schulleitungen-in-sachsen-anhalt/, Abrufdatum: 26.07.2019.

Das Schulnetz sollte aus Gründen der Skalierbarkeit und des Schutzbedarfs der in ihm kommunizierten Daten und Ressourcen in unterschiedliche Arbeitsbereiche bzw. Zonen (Level) aufgeteilt werden (siehe auch Abschnitte 3.3.1 und 3.3.4). Die Zonen (Level) sollten ggf. bei Neueingliederung weiterer Netzwerkteilnehmer weiter aufgeteilt werden. Deshalb wird im Folgenden in zwei Bereiche unterschieden:

• Nutzung digitaler Medien und Werkzeuge im Unterricht – Ausstattung Level 2

• Digitalisierung des Gebäudes – Infrastruktur Level 0 und 1

Dazu wird im Level 0 sämtliche Infrastruktur zusammengefasst, welche mit der Bereitstellung der Netzwerkinfrastruktur und deren Absicherung im Sinne der IT-Sicherheit für alle vernetzten Komponenten beauftragt ist. Dies schließt die in den nachfolgenden Abschnitten aufgeführte Firewall ein. Der Netzzugang wird auf diesem Level auch extern erreichbaren Datenspeichern (z.B. emuCLOUD) kontrolliert ermöglicht. Auch Gebäudeinfrastruktursysteme, wie z.B. Aufzugssysteme, Alarmanlage, ggf. Saugroboter etc., welche einen Netzzugang benötigen, sind über dieses Level eingebunden.

Für lokal in der Schule vorgehaltene Daten werden im Level 1 Serversysteme bereitgestellt, welche z.B. Mediendaten aber auch Datenbanksysteme enthalten können. Falls Virtualisierungslösungen zukünftig angestrebt werden, sind diese ebenfalls in diesem Level anzusiedeln.

Die eigentliche Schnittstelle zum Nutzer pädagogischen Netz und dessen Arbeitsstationen repräsentiert das Level 2. Hier sind die pädagogischen Anwendungen und Multimediasysteme verortet. Am Anfang wird zuerst der Schwerpunkt auf das Gesamtbild gelegt, um ein Verständnis für die übergeordneten Zusammenhänge zu erzeugen und Verantwortlichkeiten besser verteilen zu können. Deshalb wird im Folgenden in zwei Bereiche unterschieden:

- Digitalisierung des Gebäudes – Infrastruktur Level 0 und 1
- Nutzung digitaler Medien und Werkzeuge im Unterricht – Ausstattung Level 2

Die Infrastruktur-Architektur stellt die unterste Ebene der gesamten Schularchitektur auf dem Level 0 dar. Sie ist geprägt durch ihre Hardware- und Netzwerkelemente.

Infrastruktur Level 1 ist geprägt durch die Grundbausteine der Informationssysteme, z.B. Betriebssysteme, Datenbanken etc.

Das Ausstattungslevel 2 ist geprägt durch das Zusammenspiel von Hardware mit der darauf installierten Software (z.B. Betriebssysteme, Anwendungssoftware, z. B. Büro-Software, Software für Fachanwendungen). In Verbindung mit den technologischen Standards (z.B. Internet-Protokolle, Datentypen etc.) ergibt sich die ganzheitliche Betrachtung einer sog. Technologie-Plattform. Die nachfolgenden Kapitel geben einige Erläuterungen zu den Hardware- und Software-Komponenten in einer modernen Schule.

3.1 Schulinterne Netzwerkinfrastruktur

Die schulinterne Netzwerkinfrastruktur bedarf einer strukturierten Verkabelung der Schulgebäude über Stockwerke bis in die einzelnen Räume (Gigabitfähig bis zum Raum). Die Infrastruktur muss gesichert und zentral verwaltbar sein (Firewall und managed Network Services). Dabei muss auf die jeweils geltenden Bestimmungen des Datenschutzes Rücksicht genommen werden. Die dem Schulnetz zugrundeliegende Netzwerkstruktur / Topologie bestimmt im Wesentlichen die Funktionalität und die Sicherheit im Netz und in den einzelnen Teilnetzen.

Folgende Entscheidungen beeinflussen die Gestaltung des Schulnetzes:

- Netze/Back-Bones
- Segmentierung in Teilnetze: Schülernetz, Lehrernetz, Verwaltungsnetz
- VLAN-Struktur: WLAN-Netze für Lehrer, WLAN-Netze für Schüler, WLAN-Netze für Gäste
- Authentifizierung und Netzzugang
- definierte Übergänge zwischen den Netzen (Firewall-Struktur)
- WLAN-Infrastruktur (Abdeckung versus Bandbreite)
- Art der Authentifizierung bzw. Campus-LAN für Schulen mit mehreren Gebäuden usw.
- Zugang zum Internet (z. B. Proxy, Filterlösungen)
- Zugang zu externen Diensten, Nutzung externer Cloud-Dienste
- Einbindung der IP-Telefonie mit Quality of Service
- Einbindung der Gebäudeautomatisierung.

Für die Schulgebäudevernetzung sind Mindestanforderungen zu erfüllen:

- Die zentralen Komponenten eines Netzwerkes (z. B. Router, Switche, Server) müssen besonders geschützt werden. Ein physikalischer Schutz ist gegeben, wenn diese Komponenten in einem separaten Serverraum oder in abschließbaren Verteilerschränken untergebracht sind.
- Die zentralen Komponenten des Schulnetzwerkes müssen gegen Manipulationen sowie vor nicht berechtigten Zugriffen geschützt sein. Konfigurationszugänge zu Netzwerk-Komponenten müssen mit starken Passwörtern versehen sein. Eine Möglichkeit der Konfiguration dieser Komponenten aus dem Pädagogischen Netz ist nicht zulässig.
- Pädagogische Netze müssen zu bestimmten Zeiten (Unterrichtsbeginn und –ende) besondere Lastsituationen bewältigen können (hohes Datenaufkommen, Vielzahl gleichzeitiger Login- bzw. Logout-Vorgänge, verstärkte Zugriffe auf Datenspeicherung).

3.2 Internet-Zugang und -Bereitstellung

Alle Schulen des Landes Sachsen-Anhalt sollen bis 2021 an das Glasfasernetz angeschlossen werden, damit sie die Möglichkeiten des digital-vernetzten Lernens optimal ausschöpfen können. Die Realisierung erfolgt im Rahmen des Aufbaus eines neuen Landesdatennetzes (ITN-XT). Innerhalb dieses neuen Datennetzes werden Sicherheitskomponenten nach dem aktuellen Stand der Technik eingesetzt. So erfolgt die Datenübertragung auf dem Übertragungsweg

grundsätzlich stark verschlüsselt mit vom BSI zertifizierten Verschlüsselungskomponenten.

Es werden seitens des Projektes „ITN-XT“ alle Schulstandorte berücksichtigt. Schulträger müssen hierzu nichts veranlassen. Bei Vor-Ort-Installationen sind jedoch Mitwirkungsleistungen hinsichtlich Zutrittsmöglichkeiten, Stromversorgung etc. notwendig. Für durch ITN-XT gestellte Glasfaseranschlüsse entstehen seitens der Schulträger keine Installations- und Betriebskosten.

3.3 Internet-Gateway / Firewall-System

Die Schule hat soweit wie möglich sicherzustellen, dass Schülerinnen und Schüler keinen Zugriff auf jugendschutzgefährdende Inhalte bekommen, z.B. durch eine Internetfilterung.

Eine Firewall ist ein System aus soft- und hardwaretechnischen Komponenten, welche Datennetze sicher koppeln können. Einer Firewall kommt eine sehr wichtige Kontrollfunktion für die Netzwerkkommunikation (oftmals an zentralen Netzübergängen) zu, da durch sie ausschließlich erwünschte Zugriffe oder Datenströme zugelassen werden. Die Bedeutung dieser Komponente erhöht sich zudem dadurch, dass neben konventionellen IT-Systemen auch mobile Endgeräte und Komponenten, welche dem Internet of Things zugerechnet werden können, aber auch externe Netzwerkspeicher wie Virtual Private Clouds (z.B. emuCLOUD) in den Netzwerkverbund eingebunden werden. Eine spezielle Firewallkomponente namens „Application Level Gateway” (ALG) kann zusätzlich zu den regelbasierten Systemen Datenströme auf Basis von Sicherheitsproxies regeln.

Zusätzlich können durch Verwendung Virtueller Privater Netzwerke (VPN) dazu verwendet werden, schutzbedürftige Daten über nicht vertrauenswürdige Netzwerke wie das Internet zu übertragen. Die Integrität und Vertraulichkeit von Daten kann dabei durch kryptographische Verfahren geschützt werden.

3.3.1 Kabelgebundenes Netzwerk (LAN)

Die Basis einer funktionierenden IT-Ausstattung ist grundsätzlich eine ausreichend dimensionierte Netzwerkstruktur. Grundlage – auch für WLAN-Ausstattungen – ist hierbei die kabelgebundene Vernetzung. Diese Netzwerk-Infrastruktur wird dabei nicht mehr nur für die Informationstechnologie genutzt, sondern auch für die Kommunikationstechnik sowie für Bereiche der Gebäude und Gebäudeleittechnik. Sie sollte daher großzügig und zukunftsorientiert geplant werden.

Bei Neu- und Umbauten müssen in allen Räumen ausreichend Netzwerkressourcen vorgesehen werden.

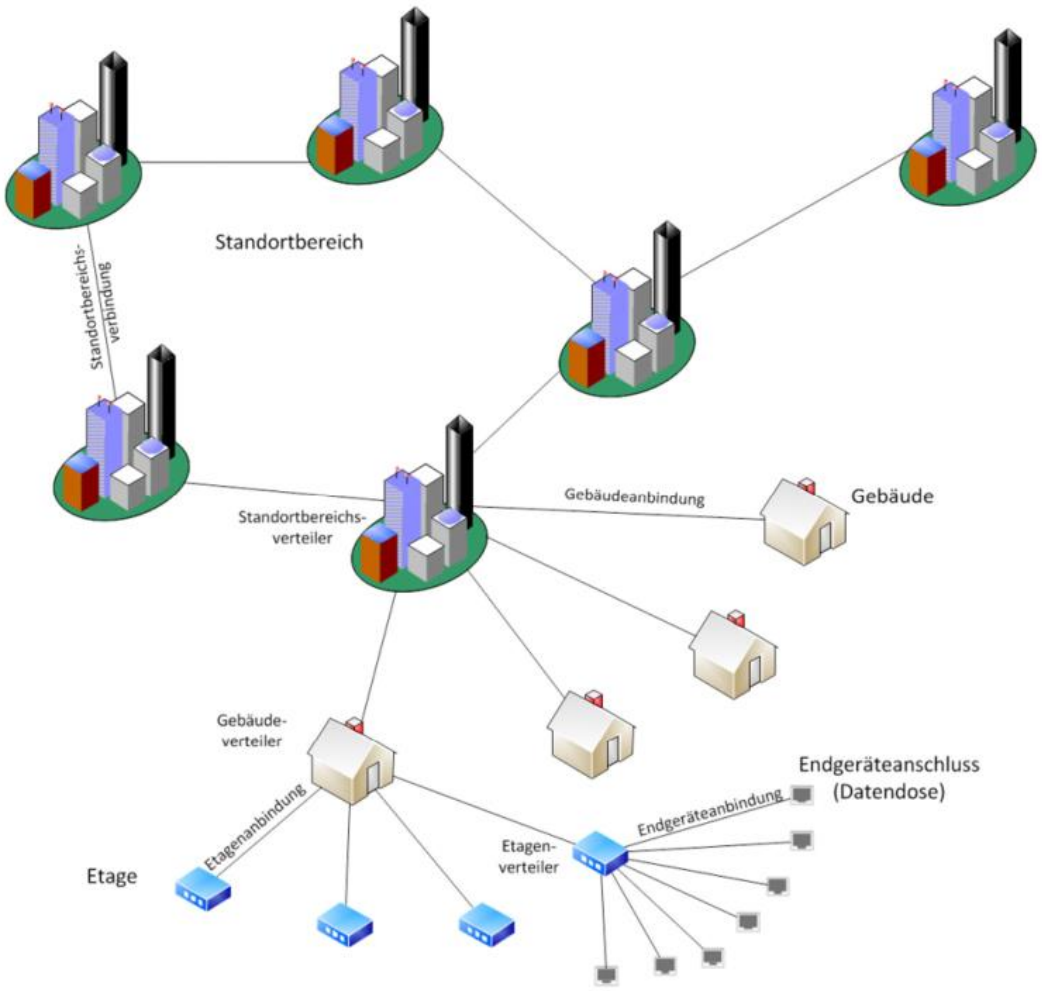


Abbildung 2 – Netzstruktur (schematisch)

Im Schulgebäude (und in den Außenstellen/Nebenstandorten/Sporthallen?) unterscheidet man regelmäßig zwischen einer Backbone-Verkabelung und der Arbeitsplatzverkabelung. Die Arbeitsplatzverkabelung (Anbindung der Clients) wird über eine Twisted-Pair-Verkabelung mit Gigabit-Ethernet-Protokoll (1 GBit / s) durchgeführt. Im Backbone-Bereich (Standortbereichs-, Gebäude-, Etagenanbindung) wird mindestens Gigabit-Ethernet (1 GBit / s) auf Lichtwellenleiter-Basis (LWL) empfohlen, je nach geplanter Nutzung kann auch eine höhere Bandbreite erforderlich werden (z. B. 10 GBit / s). Für die Anbringung von WLAN-Access-Points sind im Deckenbereich Netzwerkdosen sowie beim Einsatz von Beamern zusätzlich Stromsteckdosen zu berücksichtigen. Einige Endgeräte (z.B. IP-Telefone) werden heutzutage über Power-over-Ethernet (PoE) nach den Standards IEEE 802.3af und 802.3at verstromt, d.h. die Spannungsversorgung erfolgt über die Kommunikationsleitung.

Hierbei ist auf eine den Verfügbarkeitsanforderungen angemessene Stromversorgung durch die Switches zu achten. Der Strombedarf muss angemessen kalkuliert werden, insbesondere dann, wenn die Anzahl der Endgeräte vergrößert oder Geräte durch Technik mit höherem Strombedarf (z.B. durch integrierte Displays) ausgetauscht werden. Weiterhin sollte sichergestellt werden, dass die PoE Funktionalität auf den entsprechenden Switches nur für die vorgesehenen Ports aktiviert wird.[26]

3.3.2 Funknetze (WLAN)

Der Einsatz mobiler Endgeräte, insbesondere Tablets oder Smartphones, ist ohne eine Funkanbindung nicht sinnvoll möglich. Ein Funknetz ergänzt die strukturierte Gebäudeverkabelung, kann diese jedoch nicht ersetzen. Für stationäre IT-Geräte ist eine kabelgebundene Anbindung an das lokale Netz zu bevorzugen.

Die Anbindung von WLAN-fähigen Clients wird über Access-Points (APs) realisiert. Der Betreuungsanteil eines WLAN-Netzes sowie die damit verbundenen Kosten sind deutlich höher als bei einer rein kabelgebundenen Vernetzung. Bei der WLAN-Ausstattung größerer Bereiche bzw. ganzer Schulgebäude (WLAN-Campus) wird der Einsatz zentral administrierbarer Systeme empfohlen.

Um eine grundlegende WLAN-Ausleuchtung zu erreichen, sollte im Vorfeld eine WLAN Site Survey durchgeführt werden. Hierbei handelt es sich um eine Besichtigung der Örtlichkeiten und Festlegung zum Standort für zentrale Ressourcen (z. B. Serverraum). Dabei wird die optimale Verteilung und Position der neuen Datenanschlüsse festgelegt.

Beim Einsatz von Laptop- oder Tabletklassen und Bring-Your-Own-Device-Szenarien ist eine kapazitätsorientierte Lösung zu bevorzugen. Hierfür ist mindestens ein AP je auszuleuchtender Lokation (Verwaltung, Klassenzimmer, Lehrerzimmer o. ä.) zu beschaffen.

[26] Siehe das BSI Dokument „Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf": www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeLeitlinien/TKAnlagen/TLSTK_II-Teil_1%E2%80%93Basiswissen.pdf?__blob=publicationFile&v=1, Abrufdatum: 05.09.2019.

WLAN-Absicherung

Der Zugriff auf das Funknetz der Schule muss abgesichert und nur autorisierten Personen möglich sein. Dies wird erreicht durch

- eine zentrale individuelle Authentifizierung (z.B. IEEE 802.1x und Radius-Server oder Hotspot-Lösung mit Captive Portal-Authentifizierung)[27]
- nur in Ausnahmefällen eine verschlüsselte Verbindung (mindestens WPA2), deren Schlüssel nur autorisierten Personen bekannt ist.

Die Absicherung des WLAN-Netzes kann ergänzt werden durch einen zeitlich begrenzten Zugang auf das Funknetz, z.B. nur während der Schulöffnungszeiten sowie eine Anpassung der Sendeleistung der APs mit eigenen Antennen, die den Zugriff nur innerhalb eines bestimmten Bereiches erlauben.

Bei der Realisierung des WLANs sind die folgenden Empfehlungen des BSI in der jeweils aktuellsten Version umzusetzen:

- „Sichere Nutzung von WLAN (ISi-WLAN, Sichere Nutzung des Internet, ISi-L)“,
- „Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte“,
- „BSI TR-03103 Sicheres Wireless LAN“,
- Maßnahmenempfehlungen des IT-Grundschutzes, insbesondere Baustein „B 4.6 WLAN“.

Gesundheitsvorsorge

Vor einer Entscheidung zum Einsatz von WLAN ist die Thematik „Elektrosmog“ und „Strahlenschutz“ zu beachten. Es wird empfohlen, in dieser Problematik Einvernehmen mit allen Beteiligten herzustellen. Das Bundesamt für Strahlenschutz (BfS) empfiehlt bspw. als Vorsorgemaßnahme, kabelgebundene Alternativen vorzuziehen, wo dies möglich ist. Darüber hinaus wird empfohlen, zur Reduzierung der Strahlenbelastung bei Tablets oder Smartphones eine WLAN-Verbindung der Mobilfunkverbindung vorzuziehen. Grundlegende Informationen zu elektromagnetischen Feldern finden Sie auf der Website des Bundesamtes für Strahlenschutz.[28]

3.3.3 Funkbrücken (Richtfunk)

Die Verbindung zu einem Gebäudeteil, das mit Kabel nicht oder nur schwer erreichbar ist, ist über eine Funkbrücke möglich. Bei Sichtverbindung können mit geeigneten Antennen mehrere Kilometer überbrückt werden.

---

[27] Dafür ist eine zentrale Authentifizierungs-Instanz für alle Lehrkräfte und die Schülerinnen und Schüler erforderlich.

[28] Siehe Bundesamt für Strahlenschutz, Elektromagnetische Felder, in: www.bfs.de/DE/themen/emf/mobilfunk/schutz/vorsorge/smartphone-tablet.html, Abrufdatum: 31.07.2019.

3.3.4 Trennung der lokalen Netze in Teilnetze

Lokale Netze können in mehrere voneinander geschützte Teilnetze unterteilt werden. Jedes dieser Teilnetze ist ein eigenes Netz, in dem eigene Sicherheitsstandards definiert werden können. Die Teilnetze können über VLANs oder über eine getrennte Verkabelung gebildet werden.

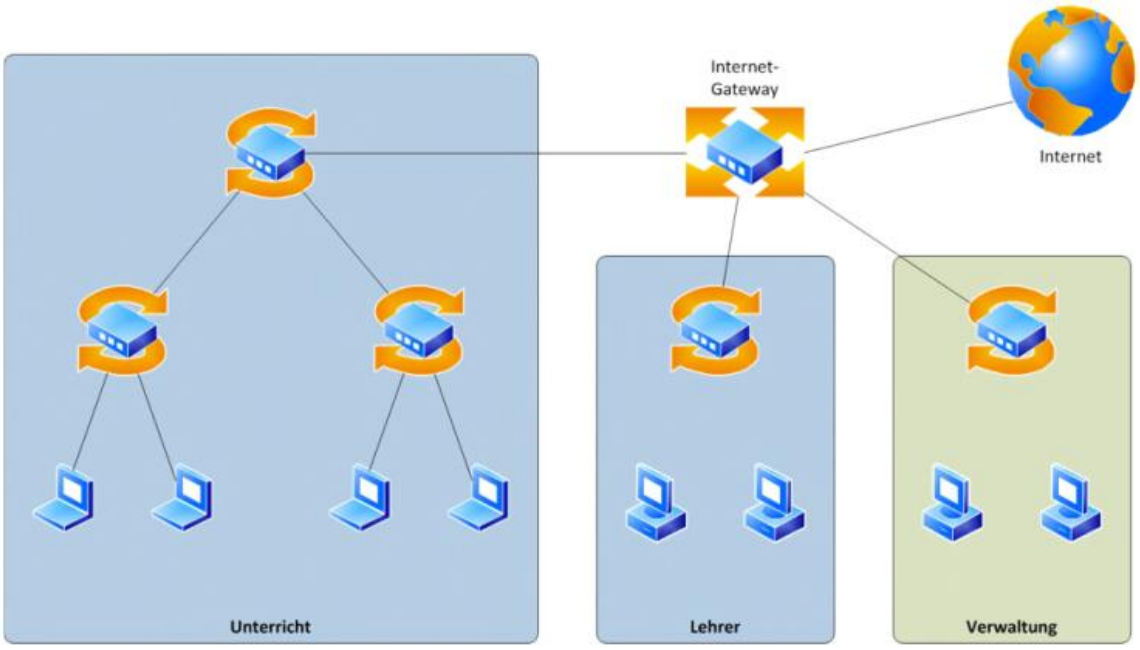


Abbildung 3 – Netzaufteilung

Zur Verbindung von Teilnetzen bzw. zur Kommunikation zwischen den Teilnetzen ist ein Router oder ein Layer-3-Switch notwendig. Damit lassen sich kontrollierbare Übergänge einrichten. Durch entsprechende Regeln wird festgelegt, zwischen welchen Netzen über welche Protokolle kommuniziert werden kann.

Hinsichtlich des Schutzbedarfes ist es notwendig, Verwaltungsbereich, Lehrerbereich und Schüler-/Unterrichtsbereich, IP-Telefonie mit Quality of Service und Gebäudeautomatisierung in verschiedene Netze zu trennen. Der Zugriff vom Schüler-/ Unterrichtsnetz auf die anderen Netze darf nicht möglich sein. Der Zugriff vom Lehrernetz auf das Verwaltungsnetz ist auf die notwendigen Verwaltungsprozesse zu beschränken. Innerhalb des Unterrichtsnetzes können weitere Teilnetze gebildet werden (z.B. Computerräume, Fachräume o.ä.). Dies ist insbesondere bei Nutzung privater Geräte (BYOD) sinnvoll.

3.4 Access-Points

Auf Grund der angestrebten Management-Vereinfachung sollte das WLAN und LAN-System der Schule auf einer einheitlichen Hardware-Plattform aufbauen.

Die Access-Points in den Schulen sind für die drahtlose Kommunikation von schuleigenen

Geräten (Notebooks, Tablets etc.) und eigenen Geräten der Schülerinnen und Schüler sowie der Lehrkräfte vorgesehen. Die APs werden in den Fluren, Klassenräumen; Aufenthalts- und Versorgungsräumen montiert. Alle APs sollen mit zwei gleichzeitig nutzbaren Radiomodulen für je 2,4 GHz und 5 GHz ausgestattet sein. Zur weiteren Unterstützung sollen die APs mehrere Netzwerke (SSID) je Signalband unterstützen. Der Anschluss der APs an das Ethernet-Netzwerk der Schule erfolgt über Datendosen mit RJ 45-Anschluss, die Stromversorgung soll in der Regel über das Datennetzwerk erfolgen (Power over Ethernet [PoE]), eine gesonderte Stromversorgung sollte vermieden werden.

Bei der Beschaffung sollte bereits auf die Möglichkeit der Erweiterung des Netzes geachtet werden (Skalierbarkeit).

3.5 Ethernet-Switche

Switches werden für die Anbindung von Endgeräten, Servern oder Netzwerkgeräten vorgesehen (Access-Switches). Es handelt sich hierbei um eine Art Vermittlungsstelle in einem Netzwerk.

Es sollen managebare Layer-2-Switche und Layer-3-Switche mit Routing-Funktionalitäten zum Einsatz kommen. Das ermöglicht den Aufbau der vorher beschriebenen virtuellen Netzwerkstruktur (VLANs) und Schaffung von Kommunikationswegen, Netzwerk übergreifend.

4. Ausstattung des digitalen Klassenzimmers

Nachfolgend wird beispielhaft die Ausstattung eines digitalen Klassenzimmers gezeigt. Diese sollten in der Schule möglichst einheitlich gestaltet sein. Die sinnvolle Nutzung der einzelnen Komponenten setzt eine entsprechende Schulung und Einarbeitung zum Erwerb der notwendigen technischen und didaktischen Kompetenzen bei den Lehrkräften voraus.

In einem digitalen Klassenzimmer verfügen Lehrkräfte über die Möglichkeit, Lerninhalte mittels Endgerät und Präsentationseinrichtung zu zeigen (Desktop-PC, Notebook oder Tablet für die Lehrkraft, Großbilddarstellung, Dokumentenkamera, Audiosystem). Schülerinnen und Schüler verfügen über digitale Geräte (z.B. PCs, Notebooks, Tablets), die sie über die schulische Infrastruktur nutzen können. Die Geräte können bei Bedarf auf einen zentral bereitgestellten Drucker zugreifen.

Zusätzliche spezielle Peripheriegeräte können in entsprechenden Förderschwerpunkten oder im Rahmen der Inklusion von Kindern und Jugendlichen mit sonderpädagogischem Förderbedarf notwendig sein. Dies betrifft besonders Ein- und Ausgabegeräte. Beispiele hierfür sind spezielle Braille-Tastaturen und -Drucker im Förderschwerpunkt Sehen, elektronische Kommunikationshilfen im Rahmen der unterstützten Kommunikation, programmgesteuerte Sprachkontrolle bzw. Bildtelefonie im Förderschwerpunkt Hören und Sprache oder programmierbare Tastaturen im Förderschwerpunkt körperlich-motorische Entwicklung.

Vielfältige Unterrichtsmethoden, die durch den Einsatz digitaler Geräte unterstützt werden

(z.B. Gruppenarbeit, Schülervortrag, Expertenpuzzle, kollaboratives Arbeiten), erfordern auch grundsätzliche Überlegungen zur Gestaltung und Möblierung der Unterrichtsräume (z.B.: Tischformen, Tablet-Aufbewahrung, Stromversorgung).

Fällt die Entscheidung für ein Nebeneinander von analoger (klassischer) Tafel und digitalem Großbild, so sollten beide von allen Schülerplätzen gut einsehbar sein. Es sollte nach didaktischen Überlegungen und praktischen Rahmenbedingungen geprüft werden, inwieweit Tafel und digitale Projektionsfläche eine räumliche Einheit bilden können, um einen Bruch im gesamten Tafelbild zu vermeiden.

4.1 Arbeitsplatz-Komponenten

4.1.1 Arbeitsplatzrechner

Sofern kein mobiler Einsatz notwendig und ein ist, kommen sog. Desktop-PC zum Einsatz.

Klassische Einsatzszenarien hierfür sind Computer-Kabinette sowie der Verwaltungsbereich der Schule. Desktop-PC sind in der Regel robuster als mobile Endgeräte. Denn sie erlauben erhöhte Wartbarkeit durch Komponentenaustausch. Aufrüstungen können bei Bedarf einfach durchführt werden und Peripheriegeräte einfach getauscht werden.

In Computer-Kabinetten soll idealerweise für jeden Schüler ein Arbeitsplatz zur Verfügung stehen. Eine Präsentationseinrichtung sowie ein Drucker sollen obligatorisch sein. Weitere Peripheriegeräte (z.B. Scanner, 3D-Drucker oder VR-Brillen) können je nach Unterrichtsinhalt ebenfalls zum Einsatz kommen.

Falls es die räumlichen Möglichkeiten zulassen, sollten die Computer so angeordnet werden (beispielsweise in U-Form), dass die Lehrkraft alle Bildschirme im Blick hat und bei Fragen der Schülerinnen und Schüler die einzelnen Arbeitsplätze schnell erreichen kann. Ergänzend sind – wenn es die räumlichen Möglichkeiten zulassen – zusätzliche Tische zur Arbeit ohne Computer sinnvoll.

In Fachräumen (z. B. Biologie, Physik, Chemie, Musik, Kunst, Werkstätten, Labore) können über die Grundausstattung des digitalen Klassenzimmers hinaus weitere (ggf. leistungsfähigere) Computer, erforderlich sein, z.B. zur Messwerterfassung, für Simulationsprogramme oder für den Videoschnitt), ebenso zusätzliche Peripheriegeräte (z. B. Funkmikrophone, Grafiktablets, Plotter).

4.1.2 Laptops

Bei der Beschaffung von schuleigenen Laptops soll auf eine robuste Verarbeitung geachtet werden. Die Akkulaufzeit sollte möglichst so ausgelegt sein, dass die Geräte weitestgehend ohne Aufladen den gesamten Schultag genutzt werden können.

Für die Aufbewahrung und den Transport der Laptops sind Lösungen in Betracht zu ziehen,

welche eine entsprechende Betriebssicherheit gewährleisten (z.B. keine Lösungen aus brennbarem Material). Zu empfehlen sind Geräte mit wechselbaren Akkus.

4.1.3 Tablets

Tablets sind mobile Endgeräte, welche über Touch-Displays angesteuert werden. Häufig verfügen diese Geräte nicht über eine eigene Tastatur. Sie bieten jedoch aufgrund ihres geringen Gewichts und der langen Akkulaufzeiten sehr gute Möglichkeiten für einen flexiblen Einsatz im Unterricht.

Die Betriebssysteme von Tablets (und Smartphones) unterscheiden sich zum Teil erheblich von denjenigen von Arbeitsplatzcomputern. Bei schuleigenen Tablets ist es sinnvoll, die Geräte in ein Mobile-Device- Management-System (MDM-System) einzubinden. Ein MDM-System sollte die vorhandenen mobilen Betriebssysteme verwalten können und folgende Funktionen bereitstellen:

- Inventarisierung von mobilen Geräten
- zentrale Konfiguration aller notwendigen Einstellungen (Desktop, WLAN etc.)
- Bereitstellung von Apps
- Sicherung bzw. Bereinigung

Die Einbindung von privaten Tablets setzt die Einwilligung der Schülerinnen und Schüler bzw. der Erziehungsberechtigten voraus.

4.1.4 Nutzereigene Geräte (BYOD)

Schülerinnen und Schüler, aber auch Lehrkräfte wollen verstärkt mit eigenen mobilen Endgeräten auch im schulischen Umfeld arbeiten (Bring-Your-Own-Device [BYOD]), denn die Verfügbarkeit digitaler Geräte als persönliche Lernwerkzeuge erweitert die Möglichkeiten der Unterrichtsgestaltung. Der Einsatz kann spontan und ohne großen Aufwand auch für kurze Unterrichtssequenzen direkt im digitalen Klassenzimmer oder an einem anderen Ort erfolgen, z.B. zuhause zur Erledigung von Hausaufgaben oder bei der Projektarbeit an einem außerschulischen Lernort.

Die Einführung von BYOD-Szenarien in einer Schule stellt allerdings erhebliche Anforderungen an die Leistungsfähigkeit und Sicherheit der technologischen Infrastruktur einer Schule. Daher ist zunächst ein BYOD-Konzept zu erarbeiten, das neben den technologischen Anforderungen (Heterogenität der Geräte, Administration, Ladeinfrastuktur) weitere Themen wie Aufbewahrung, Versicherungsschutz, Haftung etc. berücksichtigt werden. Insbesondere ist darauf zu achten, dass datenschutzrechtliche Belange nicht verletzt werden (z. B. durch Zugriffe von Apps auf persönliche Daten der Schüler oder Erfassung der Nutzungsdaten durch Anbieter).

Aus didaktischen Gründen sollte angestrebt werden, dass sich beim Einsatz digitaler Werkzeuge im Durchschnitt höchstens zwei Schülerinnen und Schüler ein Gerät teilen. Für regelmäßiges, flexibles und nachhaltiges Arbeiten mit digitalen Medien bedarf es einer 1:1-Ausstattung (z.B. schülereigene Geräte).

4.1.5 Arbeitsplatz mit Präsentationseinrichtung

Zu Demonstrationszwecken und anderen Präsentationen für den Unterricht ist eine Großbilddarstellung notwendig. Damit lässt sich der Computer über die Projektions- bzw. Bildfläche bedienen oder man kann diese wie eine digitale Schreibfläche benutzen.

Dabei kommen folgende Geräte zum Einsatz:

- PC oder Laptop,
- Soundsystem,
- Dokumentenkamera (Visualisierer),
- Beamer mit Projektionsfläche
- interaktive Whiteboards mit Touch-Funktion
- interaktive Touch-Displays.

Die Dokumentenkamera (Visualisierer) wird mit dem Projektionsgerät verbunden und ersetzt die klassischen Overhead-Projektoren. Dokumentenkameras können zusätzlich mit PC oder Laptop verbunden werden.

Sollen Präsentationen über ein Tablet oder Smartphone erfolgen, wird eine so genannte Screensharing Technologie, ein sog. Display-Adapter benötigt. Üblich sind hier z.B. Miracast, Apple AirPlay oder Microsoft Display Adapter. Bei der Anschaffung von Geräten zur Großbilddarstellung sollte darauf geachtet werden, dass die genannten Technologien unterstützt werden und keine feste Bindung an ein bestimmtes Hersteller-Ökosystem zur Folge haben.

Lehrkräfterechner

Der Rechner einer Lehrkraft muss vielseitig einsetzbar sein. Es ist darauf zu achten, dass der Rechner ohne zusätzliche Hilfsmittel mit allen anderen digitalen Peripheriegeräten (z. B. Whiteboard, Touch-Display, Beamer, Drucker etc.) der Schule interagieren kann und die pädagogische Software (Programme, elektronische Bücher, Internetanwendungen, Lernplattformen etc.) vollumfänglich funktionsfähig ist.

Interaktive Whiteboards/interaktive Touch-Displays

Mit interaktiven Whiteboards / Touch-Displays haben die Lehrkräfte die Möglichkeit, den PC oder Laptop über die Projektionsfläche zu bedienen oder die Projektionsfläche wie eine digitale Schreibtafel zu nutzen.

Dokumentenkamera

Eine Dokumentenkamera, über VGA oder HDMI mit dem Projektionsgerät verbunden oder per

WLAN[29] eingesetzt, ermöglicht die direkte Darstellung von Textvorlagen, Bildern und auch dreidimensionaler Gegenstände. Es lassen sich damit auch Abläufe aufzeichnen (z. B. physikalische oder chemische Versuche), gegebenenfalls digital bearbeiten und in Teilschritten wiedergeben. So können z.B. Erklärvideos entstehen.[30]

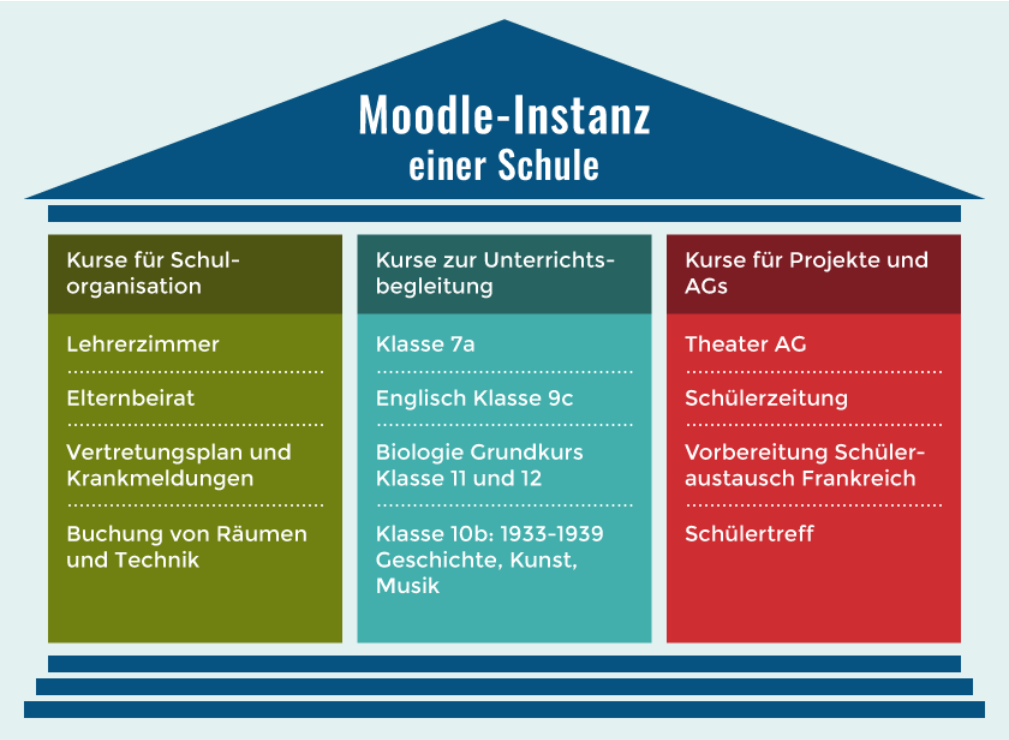
Die Funktionalität einer Dokumentenkamera kann im Prinzip auch mit einem Tablet mit geeignetem Stativ und dem Einsatz einer diesbezüglichen App erreicht werden.

4.2 Lernplattform

Lernplattformen stellen eine virtuelle Arbeitsumgebung zur Unterstützung und Organisation des Unterrichtsgeschehens dar und ermöglichen digitale kooperative Lehr- und Lernmethoden einfach in den Unterricht einzubinden und Schulorganisation zu erleichtern. Moodle ist eine solche Lernplattform, die für Sachsen-Anhalts Schulen durch das LISA bereitgestellt wird. Moodle ermöglicht es, das Lernen, Üben und Kommunizieren zeit- und ortsunabhängig in einem geschützten Bereich im Internet zu gestalten. Den registrierten Nutzern sind stets nur die für sie vorgesehenen Inhalte zugänglich und alle persönlichen Nutzerdaten und Eingaben werden nicht im Internet veröffentlicht.

[29] Das ist vorteilhaft, weil häufig genutzte Steckverbindungen Geräte außer Funktion setzen.

[30] Siehe Robert A.W. Neumann: Stop-Motion-Technik – Kurzfilmdreh mit dem Handy, in: Digitale Medien und Werkzeuge nutzen, Beispiele aus Sachsen-Anhalt, hrsg. vom Ministerium für Bildung, Magdeburg 2019,S. 18f.



Als Open Source Software ist Moodle frei verfügbar und kann an zielgruppenspezifische Bedürfnisse angepasst werden. Bildungseinrichtungen wie Schulen mit einer eigenen Moodle-

Lernplattform können daher ihre Inhalte, Funktionalitäten sowie das Design individuell einrichten, anpassen und weiterentwickeln.

Verfahren für die Bereitstellung der Lernplattform Moodle für Schulen in Sachsen-Anhalt:

- Eine E-Learning-begeisterte Lehrkraft einer Schule lässt über die Schulleitung ein Abrufangebot buchen: „schnuppern@moodle".
- Ein Mitglied des selessa-Teams demonstriert in einem Workshop in der Schule die Möglichkeiten des Systems.
- Eine bzw. mehrere interessierte Lehrkräfte lassen sich vom selessa-Team (lisa-selessa@sachsen-anhalt.de) für die Webschule freischalten, um aktuell zum Projektfortgang informiert zu werden und auf Termine zurückgreifen zu können.
- Interessierte Kolleginnen und Kollegen nehmen an Online- und/oder Präsenzfortbildungen teil, um „Moodeln" zu lernen. Aktuelle Termine und Informationen finden Sie auf dem Bildungsserver.
- Interessierte Lehrkräfte beginnen auf einer zentralen Moodle-Plattform (Einsteiger) mit ihren Schülern zu arbeiten, bis (zu einem zentralen Termin) neue Schul-Instanzen eingerichtet werden. Voraussetzung dafür ist, dass mindestens drei Kolleg*innen ebenfalls mit Moodle arbeiten und zwei davon die Moderation und Administration der Schulplattform übernehmen wollen. Auf diese Aufgabe werden die Kolleginnen und Kollegen in einer weiterführenden Fortbildungsveranstaltung vorbereitet.

5. Weitere Einsatzbereiche von IT-Technik

5.1 Unterrichtsbezogene Nutzung von frei zugänglichen Computern

Arbeitsinseln, Schulbibliotheken, Lernlandschaften oder Aufenthaltsräume können durch eine entsprechende IT-Ausstattung mit WLAN- und Internetzugang ergänzt werden. Die Schülerinnen und Schüler nutzen diese Orte außerhalb des regulären Fachunterrichts zu schulischen Zwecken, z.B. zur Recherche, zur Vorbereitung von Referaten oder zur Arbeit mit Lernplattformen.

5.2 Lehrerzimmer

Wenn im Lehrerzimmer Computerarbeitsplätze mit Internetzugang, Drucker und Scanner (üblicherweise als Multifunktionsgeräte) eingerichtet sind, erleichtert dies die Unterrichtsvorbereitung, den Informationsaustausch und administrative Aufgaben.

5.3 Ausstattung für die Seminarausbildung

Räume, die üblicherweise für den Lehrbetrieb im Rahmen der Seminarausbildung genutzt werden, sollen mindestens der Ausstattung eines digitalen Klassenzimmers entsprechen. Dies beinhaltet einen Lehrerarbeitsplatz (Desktop-PC, Notebook oder Tablet), eine Präsentationseinrichtung (Großbilddarstellung, Dokumentenkamera, Audiosystem) und die Möglichkeit, eigene digitale Geräte anzuschließen und zu nutzen.

Zudem ist eine darüberhinausgehende Ausstattung (z. B. Tabletwagen) sinnvoll, die es ermöglicht, digital gestützte Unterrichtsszenarien mit unterschiedlichen Geräten vorzustellen und praktisch zu erproben.

Seminarveranstaltungen an wechselnden Orten (z. B. im Grund-, Mittel- und Förder- schulbereich) sollten ebenfalls die Möglichkeit bieten, digital gestützte Unterrichtsformen zu erproben. Dies erfordert gegebenenfalls eine transportable Grundausstattung für ein digitales Klassenzimmer.

Ebenso ist es sinnvoll, an ausgewählten Standorten, z.B. an Medienzentren und in Referenzschulen digitale Labore einzurichten, in denen der Umgang mit unterschiedlichen Geräten erprobt werden kann.

5.4 IT-Systeme in der Schulverwaltung

Über den unterrichtlichen Bereich hinaus ist der IT-Einsatz auch zur Unterstützung der Schulverwaltung von erheblicher Bedeutung. Das Bildungsmanagementsystem Sachsen-Anhalt ist ein Softwaresystem für die Unterstützung sämtlicher Verwaltungs-, Planungs- und Statistikprozesse für Schulen, Schulbehörden und weitere an schulischen Prozessen beteiligte Einrichtungen des Landes Sachsen-Anhalt. Es wird zu spürbaren Entlastungen in den Verwaltungsaufgaben an den Schulen und in den Verwaltungen führen, so dass sich Lehrkräfte und Schulleitungen stärker auf die pädagogischen Fragen des Schulalltags konzentrieren können.[31]

[31] Über den Stand der Umsetzung informiert https://bildung.sachsen-anhalt.de/bildungsmanagementsystem-bms/startseite-bms/, Abrufdatum: 29.07.2019.

6. Software

6.1 Standardsoftware, Branchensoftware, Pädagogische Software

Vor der Beschaffung einer Software sollten die gesamten damit verbundenen Ressourcen und Kosten betrachtet werden (z. B. Installation der Software, Schulung der Lehrkräfte, ggf. notwendige Supportverträge mit dem Hersteller, Wechselwirkungen mit anderer Software).

Für Standardanwendungen ist in großem Umfang freie oder für die Schulen kostenlose Software erhältlich, die in der Regel den Anforderungen der Schule genügt.

Vor allem an beruflichen Schulen muss bei der Auswahl der Software gegebenenfalls auf die Belange der Ausbildungsbetriebe Rücksicht genommen werden.

Die Installation von Software in einem Schulnetz ist ein komplexer und zeitaufwändiger Vorgang. Vor allem die Anpassung aller Arbeitsplatzsysteme an eine neue Software kann problematisch werden. Empfohlen wird hierzu die Einrichtung eines Modellarbeitsplatzes und dessen Image entsprechend zu klonen.

Mobile Device Management (MDM)-Software kann dabei helfen, größere Mengen an Geräten zentral und einheitlich zu verwalten. Sie bildet hierbei die Grundlage zur Verwaltung von mobilen Endgeräten wie Tablets und Laptops.

So genanntes Unified Endpoint Management (UEM) kann bei sehr großen Mengen an zu verwaltenden Geräten helfen, eine einheitliche Verwaltung von Geräten aller Art (Desktop-Rechner, Server oder mobile Geräte) sicherzustellen.

6.2 Cloudbasierte Software

Anstatt Software lokal zu installieren, gibt es auch die Möglichkeit cloudbasierte Software zu verwenden, die üblicherweise als Browseranwendung läuft. Um diese zu nutzen benötigen alle Geräte eine stabile Internetverbindung.

Cloudbasierte Software bietet besondere Möglichkeiten der Zusammenarbeit (z.B. gemeinsame Datenablagen, Kalender oder Kommunikationswerkzeuge). Online-Office- Lösungen ermöglichen darüber hinaus auch die gleichzeitige Bearbeitung gemeinsamer Text-, Tabellenkalkulations- oder Präsentationsdokumente. Die Dateien der Benutzer liegen dabei auf einem zur Verfügung gestellten Onlinespeicher.

Cloudbasierte Produkte sind datenschutzrechtlich anspruchsvoll. Vor der Entscheidung für ein Produkt sollte daher immer geprüft werden, ob die vorgesehene Verwendung datenschutzkonform möglich ist.

6.3 Lernprogramme

Bei Lernprogrammen unterscheidet man lokal bzw. serverbasiert installierte Softwareprodukte, webbasierte Lernprogramme und Lernplattformen. Installierte Programme stehen auch ohne Internetverbindung zur Verfügung, erfordern aber Administrationsaufwand. Dieser Aspekt fällt bei Onlineanwendungen weg. Viele Lernprogramme stehen als Apps für mobile Geräte in den App-Stores zur Verfügung.

Ist zum Einsatz von Lernprogrammen eine Registrierung notwendig oder werden personenbezogene Daten verarbeitet, sind die datenschutzrechtlichen Bestimmungen zu beachten.

6.4 Betriebssysteme

6.4.1 Arbeitsplatzbetriebssysteme

Die klassischen Betriebssysteme für Arbeitsplatzcomputer sind Windows, Linux oder MacOS, wobei Windows[32] an den Schulen am weitesten verbreitet ist. Bei diesen Betriebssystemen stehen alle in der Schule üblichen Standardanwendungen zur Verfügung. Linux stellt eine Alternative zu Windows dar und bietet für alle Standardanwendungen freie Software an. Auch fächerspezifische Lernprogramme stehen unter Linux in großer Zahl zur Verfügung.

Bei Neuanschaffungen von PCs sollte auch ein aktuelles Betriebssystem zum Einsatz kommen, da hier die geringsten Probleme mit Gerätetreibern und Anwendungsprogrammen zu erwarten sind. Für einige ältere Systeme werden keine neuen Sicherheitsupdates angeboten, deshalb muss in besonderer Weise darauf geachtet werden, dass sie keine Viren oder andere Schadsoftware verbreiten (siehe Anhang A).

Folgende Maßnahmen tragen dazu bei:

- Betrieb der Geräte nur in einem internen Netz hinter einer konfigurierten Firewall[33]
- Nutzung eines aktuellen, datensparsam konfigurierten Internet-Browsers (siehe Anhang A)
- Betrieb der Geräte mit einer Protektor-Lösung, die nach jedem Neustart alle Veränderungen verwirft (Schutz der Arbeitsplatzcomputer vor Veränderungen)
- Bereitstellung eines sauberen System-Images und regelmäßiges Klonen der Geräte.

6.4.2 Serverbetriebssysteme

Üblicherweise sind die Clients in ein Netzwerk eingebunden und können in diesem Netzwerk zentrale Dienste eines Servers nutzen. In Betracht kommen hierbei primär Linux- oder Windows-Server. Bei allen Serverbetriebssystemen sind fundierte Kenntnisse zu deren Struktur, zu deren Administration sowie zum Aufbau des Rechtesystems notwendig.

Als Fileserver (Datenablage oder Dateiaustausch) und ggf. auch für weitere Serverdienste (z.

[32] Siehe dazu https://lfd.niedersachsen.de/download/144339, Abrufdatum: 17.09.2019.
[33] Siehe Hinweise in Anlage A.

B. Webserver, Medienserver) eignen sich auch NAS-Systeme (Network Attached Storage). Die Administration einer NAS-Box erfolgt über eine Weboberfläche und ist sehr viel einfacher als bei einem traditionellen Server.

6.4.3 Virtualisierung von Server-Systemen

In vielen Schulnetzen sind mehrere Server im Einsatz. Diese Server werden heute am sinnvollsten als virtuelle Maschinen betrieben (z.B. auf einer ESXi-, HyperV-oder Xen-Host). Dies spart erhebliche Ressourcen und erleichtert die Administration der Server-systeme. In einer VLAN-Infrastruktur lassen sich die einzelnen virtuellen Server unterschiedlichen VLANs zuordnen (z.B. Unterrichtsnetz, Verwaltungsnetz). Für die Administration von Serversystemen sind explizite Kenntnisse erforderlich.

7. IT-Systemlösungen für Schulen

Auf dem Markt wird eine Reihe von IT-Systemlösungen für Schulen angeboten, die alle gewünschten Funktionalitäten für Schulen abdecken sollen. Jedoch sind diese Lösungen zum Teil äußerst komplex und erfordern einen gesonderten Aufwand für Systembetreuer und Schulträger. Der finanzielle Aufwand für solche Lösungen ist ebenfalls nicht zu unterschätzen.

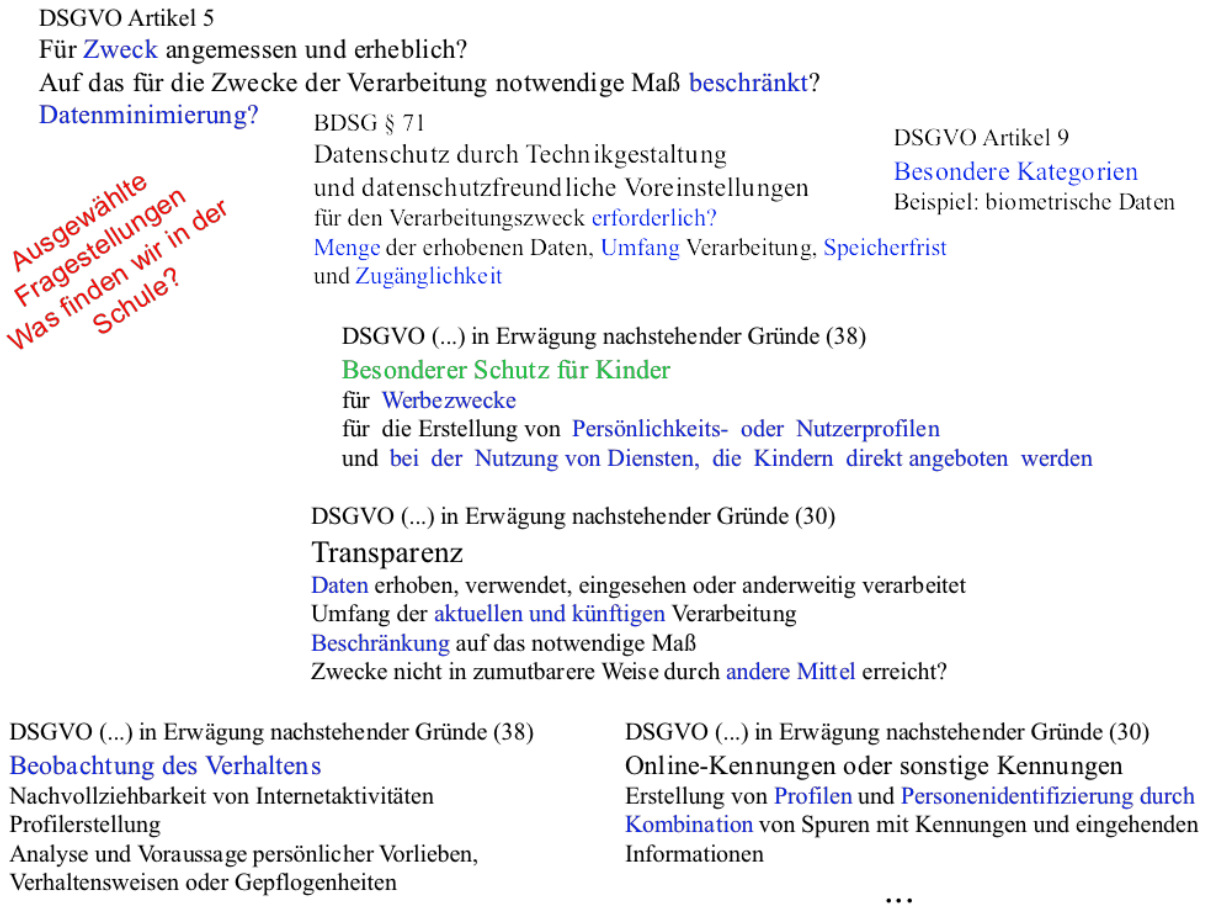
Solche Systemlösungen sollten erweiterbar sein und moderne Konzepte und Vorstellungen der Schulen (z. B. Integration von mobilen Endgeräten) nicht behindern. Vor Beschaffung solcher Systemlösungen ist daher zu prüfen, welche Funktionalitäten für die Schule notwendig sind und ob der daraus resultierende Folgeaufwand gerechtfertigt und finanzierbar ist. Zudem ist es bei Beschaffung solcher Lösungen von Vorteil, wenn mehrere Schulen im Zuständigkeitsbereich des Schulträgers sich für ein solches System gemeinsam entscheiden, um skalierbare Effekte zu erzielen.

Anlage A Empfehlungen zum Umgang mit datenschutzrelevanten Daten an der Schule

Anhang A folgt aus der Digitalen Agenda Sachsen-Anhalt und soll helfen bei der Gestaltung der Digitalisierung stets die Menschenwürde, die Unverletzlichkeit der Persönlichkeitsrechte und die digitale Souveränität der Schulen und aller Akteure zu berücksichtigen. In Digitalisierungsprozessen ist die Sicherheit der Datenspeicherorte und der Datenübertragungsinfrastruktur ein hohes Gut. Datenschutz und Informationssicherheit sind zentrale Faktoren für die gesellschaftliche Akzeptanz und den Erfolg des digitalen Wandels. Sichere Grundprinzipien der Technikgestaltung sind nicht nur ein Wettbewerbsvorteil für Unternehmen, sie bilden auch das Fundament für Datensicherheit und Datenschutz in der Schule im Sinne des besonderen Schutzbedürfnisses von Kindern. Die bewusste Auswahl und gezielte Gestaltung von Technik ist notwendiges Fundament der Mediennutzung in der Schule. Sie fördert Medienkompetenz und digitale Souveränität über die Schule hinaus. Technikgestaltung kann bereits bei der Konfiguration beginnen.

Exemplarisch sollen die folgenden Zusammenstellungen und Tabellen Denkanstöße, Hilfestellungen und Orientierung mit einer Auswahl an Techniken geben und die schulischen Akteure auf einem sicheren Weg im Netz begleiten.[34]

[34] Siehe auch Digital Safety Compass: www.klicksafe.de/service/aktuelles/news/detail/neu-bei-klicksafe-digital-safety-compass/ und www.klicksafe.de/themen/datenschutz/privatsphaere/tipps-zur-digitalen-selbstverteidigung/ 3.9.2019, Kompass für Digitale Selbstverteidigung: „Hilf Dir selbst - digitale Selbstverteidigung 4.0“ https://omen.cs.uni-magdeburg.de/itiamsl/deutsch/secbydesign/index.html 3.9.2019, Digitale Selbstverteidigung vom TLfDI https://www.tlfdi.de/mam/tlfdi/info/digitale_selbstverteidigung_05-2018_web.pdf und https://www.tlfdi.de/mam/tlfdi/digitale_selbstverteidigung__anleitung.pdf, 3.9.2019, Mike Kuketz https://www.kuketz-blog.de/empfehlungsecke/ und https://www.kuketz-blog.de/digitale-selbstverteidigung-was-ist-das-eigentlich/, 3.9.2019)



Es werden in Anlage A folgende Bausteine[35] behandelt:

- Betriebssystem
- Internetbrowser
- Suchmaschinen
- Nutzung von Apps
- Büroanwendungen (Office)
- Internet-Gateway / Firewallsystem
- Soziale Netzwerke, Chat, Messenger, Navigationsdienste
- Passwortwahl
- E-Mail
- Schulwebauftritt

[35] Ergänzend wird verwiesen auf: Kompass für Digitale Selbstverteidigung, hrsg. von der Otto-von-Guericke-Universität, Fakultät für Informatik, Magdeburg 2019, Download: https://omen.cs.uni-magdeburg.de/itiamsl/deutsch/secbydesign/index.html, Abrufdatum: 31.07.2019.
Die Inhalte sind vor dem Hintergrund der Informatik erstellt und mit größter Sorgfalt recherchiert. Es kann dennoch keine Haftung für die Richtigkeit, Vollständigkeit und Aktualität der bereit gestellten Informationen übernommen werden. Die Informationen sind insbesondere auch allgemeiner Art und stellen keine Rechtsberatung im Einzelfall dar. Zur Lösung von konkreten Rechtsfällen konsultieren Sie bitte unbedingt vorher einen Rechtsanwalt. Die Benutzung dieser Leitlinien erfolgt ausschließlich auf eigenes Risiko.

Betriebssystem

Exemplarische Auflistung von datenschutzrelevanten Daten und Gerätezugriffen des Betriebssystems für den Einsatz im Klassenzimmer

Eingabe- und Freihanddaten: Texte können individuelle Merkmale aufweisen, Texte können direkten oder indirekten Personenbezug haben.

Mikrofondaten: Aufnahme von Sprachdaten zur Sprach- und Sprechererkennung erleichtert direkte Personenidentifizierungen, da Personen sich mit Namen ansprechen und entsprechend antworten (wie Schüler, Eltern und Lehrkräfte). Aufgenommene Sprachdaten erlauben Bestimmung von emotionalen Zuständen oder des Gesundheitszustandes der in Reichweite des Mikrofons befindlichen Personen (im Raum oder in der Nähe des Raumes).

Kameradaten: Aus der Aufnahme vom Gesichtsbild und weiterer visueller biometrischer Merkmale einer Person (wie Handgeometrie, Gang, Ohr), die in anderen Geräte-/Betriebssystem-Nutzungen oder Internetquellen bereits mit direktem Personenbezug verfügbar sind oder zukünftig verfügbar werden, kann ein emotionaler Zustand oder Gesundheitszustand abgeleitet werden.

Diagnose- und Telemetriedaten umfassen System- und Nutzungsinformationen[36], wie beispielsweise) und enthalten in den Standardeinstellungen viele sensible Daten, aus denen auch biometrischer Daten abgeleitet werden können (wie Handwriting, Pen-Gesture oder Palm-Touch, Surf-Verhalten, Suchanfragen, emotionale Zustände, Gesundheitseinschränkungen, etc.) und werden oftmals auch an Dritte übertragen, direkter Personenbezug kann durch Kombination mit anderen Geräte/Betriebssystem-Nutzungen oder Internetquellen erfolgen.

Gerätezugriffe auf Mikrofon, Kamera und Positionsdaten: Die genannten Geräte ermöglichen Datenerhebungen, -übertragungen und -speicherung und bergen die Gefahr zur Beobachtung des Verhaltens und Erstellung von Profilen und Personenidentifizierung durch Kombination von Spuren mit Kennungen und eingehenden Informationen.

Zusätzlich verwendete Sensoren bergen ebenfalls erhöhte Risiken (3D-Brillen, Infrarotkameras, Augen-Überwachungen usw.).

Hinweis: Die Auflistung enthält die in einem heutigen Standard-Gerät zu erwartenden Medien. Offensichtliche Daten mit Personenbezug sind nicht explizit benannt.[37]

[36] Siehe am Beispiel von Windows 10 zusammengefasst vom Bundesamt für Sicherheit der Informationstechnik: SiSyPHuS Win10: Analyse der Telemetriekomponenten in Windows 10, https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/SiSyPHuS_Win10/AP4/SiSyPHuS_AP4_node.html, Abrufdatum: 30.07.2019.

[37] Siehe hierzu die Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, Download: https://www.datenschutzkonferenz-online.de/media/oh/20180426_oh_online_lernplattformen.pdf, Abrufdatum 18.01.2019.

Betriebssystem

Leitlinien zum Umgang mit dem Betriebssystem

Grundsatz: Nutzen Sie datensparsame Betriebssysteme bzw. konfigurieren Sie das Betriebssystem datensparsam. Beachten Sie dabei folgende Hinweise.

1. Geräteaktivierung (Mikrofon, Kamera)	Sensoren, wie Mikrofon und Kamera, die Nutzer aufnehmen, inaktiv schalten oder ganz deaktivieren (Anschalten im Bedarfsfall für eine Anwendung, Ausschalten nicht vergessen!)
2. Bluetooth etc.	Im Default alle nicht dringend benötigten Netzverbindungen oder automatische Verbindungen deaktivieren, angebundene Geräte explizit mit entsprechenden Sicherheitseinstellungen einbinden (Anschalten im Bedarfsfall für eine Anwendung, Ausschalten nicht vergessen!)
3. Telemetrie und Diagnose	keine Telemetriedaten erheben und versenden, Telemetriedienste deaktivieren und Diagnose auf sicherheitsrelevante Angaben reduzieren, Diagnosedaten-Viewer installieren und Option „Diagnosedaten anzeigen“ aktivieren, um partielle Transparenz herzustellen Achtung: zunächst prüfen, ob Diagnosedaten-Viewer ohne Microsoft Konto ladbar ist - ansonsten Potential für unerwünschten Datenabfluss und ungewollte Verknüpfungen
4. Clouddienste	lokale oder Schuldienste aus Sachsen-Anhalt (wie z.B. bildung-lsa.de und emuCloud) nutzen statt Drittanbieter-Cloud oder Drittanbieter-Lösungen; ggf. auf öffentlich-rechtliche Cloudanbieter und private Cloudanbieter mit Sitz in der EU zurückgreifen[38]
5. Sprach- und Sprechererkennung	keine externe Sprach- und Sprechererkennung nutzen, bei Vorhandensein deaktivieren, lokale Ansätze nutzen (siehe z.B. snips: https://snips.ai/)
6. Anti-Virus-Programme	sicherstellen, dass keine Versendung von Daten an den Anbieter/Hersteller/Dritte erfolgt, lokale Installation auf Schulrechner/Schulserver
7. Datensicherungen / Backup	regelmäßige lokale Datensicherungen mit Versionsverwaltung auf nur kurzzeitig angeschlossenen Systemen durchführen zum Schutz vor Computerviren (Schadcode) wie Ransomware[39]

[38] Dies ist keine datensparsame Variante, da Verbindungsaufbau und Netzaktivitäten zum Drittanbieter sichtbar und auswertbar werden. Zum schulischen Datenschutz siehe auch Fragen und Antworten für Lehrkräfte in Rheinland-Pfalz, in: www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Publikationen/flyer-schulischer-datenschutz.pdf, Abrufdatum: 31.07.2019.

[39] Siehe Bundesamt für Sicherheit in der Informationstechnik: Datensicherung, www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/CON/Umsetzungshinweise_zum_Baustein_CON_3_Datensicherungskonzept.html, www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Datensicherung/datensicherung_node.html, /www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Datensicherung/datensicherung_node.html, Abrufdatum: 30.07.2019.

8. Benutzerauthentifizierung	für sicherheitskritische Rollen/Benutzer Mehrfaktorauthentifizierung verwenden
9. Verschlüsselung	Verschlüsselungen auf Anwendungsebene für personenbezogene Daten/Dokumente (ggf. verschlüsseltes Dateisystem oder Ordner) und standardmäßig auf Netzebene aktivieren

Betriebssystem
Leitlinien zum Einsatz von Windows 10 im Klassenzimmer

Grundsatz: Windows 10 ist aktuell das am häufigsten eingesetzte Betriebssystem. Dieses setzt jedoch nicht Privacy by default um. Wer es an Schulen einsetzen will, muss im Sinne des Datenschutzes auf eine datenarme Konfiguration[40] achten. Dabei sind die nachfolgenden Hinweise hilfreich.

1. Betriebssystem setzt „Privacy by Default“ um	Benutzerdefinierte Installation erforderlich, d.h.: (Stand hier entsprechend: Windows 10 1703 und 1803) Es müssen alle relevanten Einstellungen per „opt-out“ auf datenschutzkonforme bzw. datenarme Einstellungen umgestellt werden. Dies beinhaltet u.a.: - Ausschalten von Funktionen über Anpassung der Einstellungen zur Personalisierung: – Ausschalten von Spracherkennung, – „Eingabe und Freihand-Personalisierung“, – „Werbe-ID für Apps erlauben“, – Skype-Adressbuchvernetzung, – Positionsdatenübermittlung einschl. Positionsverlauf), – Verbindungs- und Fehlerberichterstattung ausschalten, – Browser-Schutz und -Update ausschalten, – Deaktivierung von Cortana, – keine Verknüpfung mit einem Microsoft-Konto (Verwendung eines lokalen Benutzerkontos), – Synchronisation von Einstellungen ausschalten, – Datenschutzoptionen ändern (Verwendung der Werbe-ID, das Senden von Informationen zum Schreibverhalten an Microsoft, den Zugriff auf die Sprachliste, SmartScreen-Filter, Deaktivierung des Protokollierens zum Öffnen und Benutzen von Apps, Deaktivieren von Microsoft-Werbung und andere Personalisierungsinfos verwalten), – Deaktivierung App-Zugriff auf: Kamera, Mikrofon, Benachrichtigungen, Spracherkennung, Freihand und Eingabe, Kontoinformationen, Kontakte und Kalender, Anrufliste, Email, Messaging und Funkempfang, Weitere Geräte,

[40] „Windows 10 verfolgt nicht das „Privacy by Default“-Prinzip, d.h. datenübermittelnde Funktionen müssen explizit deaktiviert werden“, so der Arbeitskreis Informationssicherheit der deutschen Forschungseinrichtungen (AKIF) – siehe: Orientierungshilfe zur datenarmen Konfiguration von Windows 10, https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf, Abrufdatum: 8.4.2019.

	– Windows 10 Taskleisten-Suchfeld deaktivieren, – Nutzung von OneDrive deaktivieren, – Edge deaktivieren bzw. datenarm konfigurieren, – Apps / Windows Store deaktivieren, – App-Benachrichtigungen deaktivieren, – Update konfigurieren (siehe z.B. „Übermittlung von Updates auswählen“ - Reduzierung unnötiger Datenerhebung: z.B. - die Einstellung auf Telemetry-Level auf “Basic” plus weitere Einstellungen wie über Policies Detailstufe auf „Sicherheit“ reduzieren bzw. möglichst den DigiTrack-Dienst vollständig deaktivieren oder die zugehörigen IP-Adressen des Microsoft-Backends umkonfigurieren auf ungültige Adressen[41] - Abschaltung von kritischem Gerätezugriff durch das Betriebssystem und alle Anwendungen, speziell: – Mikrofon, – Kamera und – Positionsdaten, die in der Standardeinstellung für alle Applikationen, die installiert werden, nutzbar sind (Achtung: separate Einstellungen für den Sperr-/Loginbildschirm sowie jeweils neu installierte Anwendungen) durch Gruppenrichtlinien (siehe [AKIF] – Seite 56 ff Anhang 1) Hinweis datensparsame Videotelefonie: Falls für den Lehreinsatz notwendig, sollten anstelle des von Microsoft angebotenen Skype-Dienstes datensparsame Videotelefonie–Dienste, wie der vom DFN, genutzt werden und die Kamera und das Mikrofon nur für diesen Dienst im Einsatz begrenzt erlaubt werden.
2. Konfigurationen zur Wahrung der Privatsphäre	Vorgenommene Konfigurationen zur Wahrung der Privatspähre sollten bei Updates nicht modifiziert werden, erfolgte Modifikationen sind wieder anzupassen Nutzung alternativer Betriebssysteme, die Privacy-Konfigurationen beibehalten.
3. Werbefreiheit	Nutzung von Windows Education Pro Lizenzen, um Einstellungen anpassbar zu haben, und Deaktivierung von Werbung vornehmen zu können
4. Clouddienste für das Speichern sensitiver Daten	Nutzung von strikt lokaler Speicherung (oder Suche) mit Eingriff in die Registry oder die Gruppenrichtlinien (findet die Speicherung und Auswertung von Daten in der Microsoft-Cloud statt, bedeutet dies, dass auch eine ständige Datenverbindung zu den Microsoft-Servern notwendig ist. Dabei muss davon ausgegangen werden, dass persönliche Daten übertragen und gespeichert werden.

[41] Nach Upgrades muss dies erneut konfiguriert werden), siehe Details unter www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/SiSyPHuS_Win10/SiSyPHuS_node.html und siehe Sandbox-Ansatz in Windows 10 in der Linux-Sandbox - Auf Nummer sicher von Lukas Grunwald, https://www.heise.de/select/ix/2019/5/1908016054629797396, Abrufdatum: 6.5.2019

5. Entkoppelung von Betriebssysteme und kritischen Anwendungen	Um die Möglichkeiten zum Nutzer-Profiling zu optimieren, arbeiten die Telemetriedienste von Microsoft-Produkten wie Windows 10, Office und Edge Hand in Hand. Hier muss durch die Nutzung von alternativen Komponenten (z.B. Mozilla Firefox als Webbrowser, Thunderbird für E-Mail mit Enigmail-Verschlüsselungsplugin) die Datensammlung durch einzelne Firmen erschwert werden.
6. Konfigurierbarkeit und Wartbarkeit von Klassenzimmerinstallationen	Nutzung von Windows 10 als Education Lizenzen für Bildungseinrichtungen mit Werkzeugen für das Roll-out von Klassenzimmerinstallationen, genaue Prüfung in Kombination mit Supportverträgen von Drittfirmen (z.T. in Koppelung mit Beschaffungs- und Wartungsverträgen) ist notwendig, alternativ zur Installation, Konfiguration und Wartung durch eigenes Personal. Die Realisierung und Konfiguration nach Vorgaben oder eigenen Vorstellungen der Firma ist durch die jeweilige Schule zu prüfen, ob u.a. für OneDrive geltenden Datenschutzrichtlinien gesetzeskonform umgesetzt wurden. Leider ist dies nicht nur zum Installationszeitpunkt notwendig, sondern aufgrund der Updatepolitik von Microsoft und - beim Umgang mit den Rechten der angelegten Nutzer auch regelmäßig im Betrieb erforderlich.
7. Microsoft Konto Kind Tracking	Microsoft-Konto mit Option “Kind“ nicht nutzen – Lehrkraft könnte Schüler/in als Kind verwalten, externe Diensteanbieter könnten ebenfalls Schüler/in als Kind verwalten.

Alternative Betriebssysteme

Grundsatz: Lernen Sie alternative Betriebssysteme für den Schuleinsatz mit Orientierung an Privacy by Design und die Nutzung von Konfigurationsmöglichkeiten kennen.

Linuxmuster	„Linuxmuster.net ist eine umfassende Komplettlösung für den Betrieb schulischer Netzwerke. Sie wird von Lehrkräften und Dienstleistern für die speziellen Anforderungen in der Schule entwickelt.“ – Komplettlösung: http://www.linuxmuster.net/de/start/ Konfigurationshilfen nutzen
Skodelinux (Debian Edu)	„Skolelinux ist nicht nur ein Softwareprojekt, sondern auch eine aktive Gemeinschaft, die freie Software für den Bildungseinsatz zusammenträgt, erprobt, dokumentiert, unterstützt und weiterentwickelt. Das passiert sowohl online als auch offline, in regionalen Arbeitsgruppen und international.“ – Skolelinux (Debian Edu) https://www.skolelinux.de/de/ Konfigurationshilfen nutzen: https://www.skolelinux.de/en/ Bei Integration von Windows-Clients müssen die Orientierungshilfen zu Windows 10 beachtet werden!
Puavo	Lösung aus Finnland, Medienkonzepte für und mit finnischen Schulen, auch in deutscher Sprache erhältlich, basiert auf OpenSource - https://github.com/opinsys Konfigurationshilfen nutzen

Leitlinien für Internetbrowser

Grundsatz: Vermeiden Sie Tracking durch Dritte sowie Werbung durch gezielte Auswahl eines sicheren und datensparsamen Browsers.[42]

1. Browserwahl	Auswahl und Konfiguration eines sicheren Privacy by Design und Default-Browsers bzw. notwendige Nachkonfiguration des Browsers; Dabei gilt es, auf Aktualisierungen zu achten! Mit PrivacyScore.org und https://webbkoll.dataskydd.net/de/ kann geprüft werden, welche Blocker und Tracker in Websites vorkommen und ob die HTTPS-Verschlüsselung eine gute Sicherheit bietet. Browser mit der Möglichkeit der Überprüfung der Implementation sind zu bevorzugen (Open-Source ermöglicht unabhängiges Programmcode-Review).
Firefox **Waterfox** **Pale Moon** **Brave** **Google Chrome** **Opera** **Edge**	empfohlen, aber Konfiguration erforderlich[43] empfohlen[44] empfohlen[45] empfohlen, aber Konfiguration erforderlich[46] aus Privacy-Sicht nicht empfohlen - https://restoreprivacy.com/secure-browser/ und https://www.kuketz-blog.de/chrome-edge-safari-und-opera-browser-mit-wenig-privatsphaere/, Abrufdatum 17.06.2019 und https://www.golem.de/news/ublock-und-privacy-badger-google-schraenkt-werbeblocker-in-chrome-ein-1906-141627.html, Abrufdatum 17.06.2019 aus Privacy-Sicht nicht empfohlen - https://restoreprivacy.com/secure-browser/ und https://www.kuketz-blog.de/chrome-edge-safari-und-opera-browser-mit-wenig-privatsphaere/ Website request 17.06.2019 und https://www.golem.de/news/ublock-und-privacy-badger-google-schraenkt-werbeblocker-in-chrome-ein-1906-141627.html, Abrufdatum 17.06.2019 aus Privacy-Sicht nicht empfohlen - Ref https://restoreprivacy.com/secure-browser/ und https://www.kuketz-blog.de/chrome-edge-safari-und-opera-browser-mit-wenig-privatsphaere/ Abrufdatum 17.06.2019
2. Browser Compartmentalization	Empfehlenswert ist die Nutzung verschiedener Browser für verschiedene Zwecke.
3. Secure Browser Add-ons	Nutzung und Konfiguration von Transparenz- und Blocking-Werkzeugen wie zum Beispiel uBlock Origin, HTTPS Everywhere, Privacy Badger, Cookie Autodelete, Decentraleyes, uMatrix, NoScript, Random User Agent oder Skip Redirect und Neat URL, siehe 5 – Die Überprüfung der Add-ons vor Nutzung ist erforderlich bzw. eine Konfiguration (block all, Datensammlung etc.) - Auf Aktualisierungen ist zu achten!

[42] Ergänzende Hinweise zur Konfiguration der einzelnen Brower im Sinne von Datenschutz, Datensicherheit und Datensparsamkeit finden Sie hier: https://restoreprivacy.com/secure-browser/, Abrufdatum: 30.07.
[43] Siehe: https://www.kuketz-blog.de/empfehlungsecke/#firefox und https://www.kuketz-blog.de/firefox-ein-browser-fuer-datenschutzbewusste-firefox-kompendium-teil1/. Abrufdatum: 31.07.2019.
[44] Siehe: https://restoreprivacy.com/secure-browser/, Abrufdatum: 30.07.2019.
[45] Siehe: https://restoreprivacy.com/secure-browser/, Abrufdatum: 30.07.2019.
[46] Siehe: https://restoreprivacy.com/secure-browser/, Abrufdatum: 30.07.2019.

4. Testen des Browsers und der Add-Ons	Zur Beurteilung des privatsphären-konformen Verhaltens von Browsern und Add-Ons können einige Werkzeuge wertvolle Hilfe nach deren Konfiguration liefern, z.B. von Panopticlick und Qualys SSL Labs[47]
5. Anonymsierungsdiensten	Anonymisierungsdienste können helfen, die eigene Präsenz zu verschleiern, z.B. https://torproject.org.
6. Inspektion von Webseiten	Empfehlenswert ist die Nutzung von Zusatzwerkzeugen zur Prüfung u.a. auf Verbindungsversuche zu Drittanbietern z.B. mit dem Webdeveloper-Plugin für Firefox-Browser
7. Startseite und neue Tabs	Beim Start des Browsers wird die Startseite bzw. bei einem neuen Tab ebenfalls eine vorkonfigurierte Seite aufgerufen. Sind diese nicht leer, wird eine Verbindung zur angegeben Seite aufgebaut, dieser Verbindungsaufbau zeigt somit die Nutzeraktivitäten an. Dies wird durch Konfiguration der Startseite bzw. einer neuen Tab-Seite auf eine Leerseite verhindert, denn so erzeugt der Browseraufruf keine Netzwerkaktivität.
8. Suchmaschinen	Verwendung und Konfiguration von datensparsamen Suchmaschinen, auf teilweise verdeckte Weiterleitung zu datenintensiven Suchmaschinen achten.

Leitlinien für Suchmaschinen

Damit Suchmaschinen suchen können, lesen und speichern sie den Suchanfragetext und die Verbindungsdaten zum Anfragenden. Enthält der Suchtext persönliche Informationen, so kann es zur direkten Identifizierung des Anfragenden kommen. Aus den Anfragen können auch Profile zum Anfragenden gebildet werden. Empfohlen wird die Verwendung und Konfiguration von datensparsamen und sicheren Suchmaschinen. Zu achten ist auf verdeckte Weiterleitung zu datenintensiven Suchmaschinen und die Deaktivierung automatischer Suchvorschläge. Die Liste der empfehlenswerten Suchmaschinen kann sich ändern - auf Aktualisierungen achten!

1. Nutzung datensparsamer Suchmaschinen	Nach aktuellem Stand datensparsame Suchmaschinen sind z.B. lite.qwant.com – sichere EU-Suchmaschine mit Ökostrom - eigener Suchindex, ggf. Rückgriff auf Bing MetaGer.de – deutsche Metasuchmaschine mit Ökostrom YaCy.net – dezentrale Suchmaschine, Verteilung der Suchanfragen auf ein P2P-artiges Netzwerk Speziell für Kinder empfohlen: blinde-kuh.de oder www.qwantjunior.com/ Achtung: Diese Empfehlung gilt nur für die direkte Suche, ggf. eingebundene Drittanbieter liefern personalisierte Ergebnisse, wie FragFinn.de auf Basis von direkter Suche in Google-Suche!
2. Konfiguration der Suchmaschine	Sowohl im Browser als auch den Suchmaschinen lassen sich Einstellungen vornehmen, hier ist z.B. empfohlen, Suchvorschläge zu deaktivieren, um eine Profilbildung zu verhindern

[47] Siehe: https://panopticlick.eff.org/ und https://www.ssllabs.com/, Abrufdatum: 30.07.2019..

Leitlinien für die Nutzung von Apps

Grundsatz: Tracking durch Dritte ausschließen, gezielte Auswahl einer Privacy by Design/Default App, datenarme Konfiguration der App, Nutzung von Transparenz- und Blocking-Werkzeugen, bevorzugte Verwendung lokaler Apps (Need-to-know)
Achtung: Dringend notwendige Vorgabe: Genereller Verzicht auf Apps mit ständig aktiviertem Mikrofon und/oder Kamera und akustischen Meldungen im Unterricht wegen Störung und Preisgabe persönlicher Nachrichten.

1. Überprüfung der App-Zugriffe	Prüfung der App-Zugriffe und Verbindungen vor dem Einsatz; datenarme Nachkonfiguration der Apps (Berechtigungen)[48]
2. Limitierung der App-Zugriffe und Datenversendung beim Einsatz	Maßnahme: vor Nutzung Rechte anschauen, prüfen, ggf. umkonfigurieren (Libraries geben oft Aufschluss) und dann entscheiden, ob datenarme Nutzung möglich ist, Tracker ggf. mit Werkzeugen blockieren wie BLOKADA.
3. Ansprech-partner in der EU	Verweis auf Marktortprinzip der DSGVO und Forderungen aus Art. 3 Abs.1 sowie Art. 27 zur Rechtewahrnehmung durch Betroffene
4. Datenschutz-anforderungen an App-Entwickler und App-Anbieter	Datenschutzanforderungen umsetzen aus den Orientierungshilfen für App-Entwickler und App-Anbieter des Bundesbeauftragen für den Datenschutz und die Informationsfreiheit[49]
5. Ortsinformationen	Ortsinformationen sind sensible Daten, falls keine dringende Notwendigkeit vorliegt (Zweck und Erforderlichkeit), so ist darauf zu verzichten und die Abfrage des Standortes auszuschalten
6. Accounts/ Kontos	In Accounts und auf Konten werden die Nutzeraktivitäten hinterlegt und können vom Diensteanbieter eingesehen und verarbeitet bzw. anderweitig genutzt werden, es besteht eine Vielzahl an Gefährdungen. Deshalb sollte man lokalen oder landeseigenen Accounts/Kontos den Vorzug geben.
7. Interfaces zu Drittanbietern	Verzicht auf bzw. Entfernung von SDKs zu Drittanbietern (u.a. Facebook SDKs)
8. Nutzung alternativer, datensparsamer App-Depots	App-Depots können viele Metadaten erfassen, einige davon können personenbezogen sein. Deshalb sollte man datensparsame Depots nutzen - z.B. F-Droid.

[48] Siehe https://exodus-privacy.eu.org/en/page/what/, Abrufdatum: 30.07.2019.
[49] Siehe https://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/orientierungshilfen-node.html, Abrufdatum: 30.07.2019.

Leitlinien für Büroanwendungen (Office)

Grundsatz: Tracking durch Dritte ausschließen, gezielte Auswahl eines Privacy by Design / Default App, datenarme Konfiguration.

1. MS Office	Cloud-basierter Einsatz wird derzeit (2019) von Datenschützern für bedenklich gehalten, Nutzung erst nach Datenschutzanalyse möglich[50]
2. LibreOffice	Empfohlene Nutzung von OpenSource und datenarmen Werkzeugen
3. DTP/CAD/ Medienproduktion	Empfohlene Nutzung von lokalen OpenSource-Anwendungen und datenarmen Werkzeugen
4. Rechtschreib- und Übersetzungsunterstützung; Vorlesedienste	Empfohlen ist die Verwendung lokal auf dem System installierter Softwarehilfen für Rechtschreibung/Übersetzung/Vorlesen, ein Transfer auf Dienste/Systeme Dritter ist zu vermeiden.
5. Clouddienste	Für den Austausch von personenbezogenen Dateien und Nachrichten werden schulinterne Cloudlösungen oder landesweite Dienste wie emuCLOUD empfohlen, ggf. auch öffentlich-rechtliche und private Cloudanbieter mit Sitz innerhalb der EU.[51]
6. Einsatz digitaler Assistenten	Digitale Assistenten mit der Verarbeitung der Daten in der Cloud sind zu vermeiden. Statt dessen sind lokal arbeitende Alternativen wie Snips (https://snips.ai/) zu verwenden.
7. Einsatz von Digitalkameras	Digitalkameras sollten keine WiFi- oder Mobilfunkanbindung besitzen, Aufnahmen (Bild, Ton, Video) lokal speichern, Achtung: Urheberschutz und Aufnahmen von Personen fallen unter das Recht am eigenen Bild.

[50] Schulischer Datenschutz - Fragen und Antworten für Lehrkräfte in Rheinland-Pfalz, in: https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Publikationen/flyer-schulischer-datenschutz.pdf, Abrufdatum: 31.07.2019.

[51] Siehe dazu: www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_3_2_Firewall.htm, www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_5_Protokollierung.html, https://www.datenschutzkonferenz-online.de/orientierungshilfen.html und https://www.datenschutzkonferenz-online.de/media/oh/20180426_oh_online_lernplattformen.pdf.

Leitlinien für Internet-Gateway / Firewallsystem

Grundsatz: Es gilt, eine datenschutzgefährdende Kommunikation zu unterbinden.

1. Betrieb von eigenen DNS-Servern	Namensauflösung unerwünschter Dienste ist zu vermeiden (lokaler Server oder zentraler Server für Schulen in Sachsen-Anhalt).
2. Einsatz von Firewalls	Datenverkehr filtern und minimieren durch Intrusion Prevention System (IPS): Schutz vor Viren, Spyware, und Würmern, HTML-, Javascript-, PDF-Virenschutz usw., Überwachung gepackter Dateien URL-Filterung: Es soll eine URL-Filterung entsprechend einer dem deutschen Jugendmedienschutz entsprechenden tagesaktuellen Liste erfolgen. Die Filterung sollte auf Nutzer, Gruppen oder MAC- bzw. IP-Adressen erfolgen. Daten-Filterung: Überwachung von nicht autorisiertem Datenverkehr (personifizierte Daten, Zahlungsdaten etc.) Application-Management: Das System soll in der Lage sein, Applikationen zu erkennen und zu prüfen sowie unverschlüsselten und verschlüsselten Datenverkehr (SSL, SSH) zu überwachen. User-Kontrolle: Zur Nutzerverwaltung bietet sich eine Schnittstelle zu einem zentralen Verzeichnisdienst an. Die Filterung muss auch dedizierte Trackingdienste umfassen, z.B. analytics.google.com; die Telemetriedatenübermittlung kann ebenfalls mit Firewalls eingeschränkt werden.[52]
3. Konfiguration von App-Zugriffen	Unerwünschte Datenausleitungen mit datenschutzrelevanten Inhalten können durch einen App-Check z.B. mit exodus-privacy.eu.org detektiert und durch Konfiguration von Firewall und Intrusion-Prevention-System sowie Namensdiensten (DNS) unterbunden werden.
4. Test und Blockieren von unerwünschten Verbindungen	Untersuchung der Verbindungsaufbauten von Betriebssystem und Applikationen aller Infrastrukturelemente mittels Paketinspektion, z.B. mit Wireshark und Konfiguration von Firewall und Intrusion-Prevention-System sowie Namensdiensten (DNS) zur Unterdrückung ungewünschter Verbindungsaufbauten.
5. Test der SSL- Sicherheit	Sowohl die eigenen Server eines Internetauftritts als auch sämtliche Klienten (inkl. Webbrowser) sollten einem ssl-Sicherheitstest unterzogen werden, um die IT-Sicherheit als Basis für Datenschutz zu erhöhen.[53]
6. Bereitstellung eigener, lokaler Serverdienste für Messenger	Für einige Messenger-Dienste z.B. Jabber, können lokale Server im LAN installiert werden und gegen Verbindung in das Internet abgesichert werden. Tests und Konfiguration sollten im Firewall-/Gatewaysystem erfolgen.

[52] Siehe dazu: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/SiSyPHuS_Win10/AP4/SiSyPHuS_AP4_node.html (Abrufdatum: 22.1.2019)
[53] Siehe https://www.ssllabs.com/ssltest, Abrufdatumg: 07.03.2019.

Leitlinien für soziale Netzwerke, Chat, Messenger, Navigationsdienste

Grundsatz: Tracking durch Dritte ausschließen, gezielte Auswahl eines Privacy by Design/Default Dienstes, datenarme Konfiguration, Nutzung von Transparenz- und Blocking-Werkzeugen, bevorzugte Verwendung lokaler Apps (Need-to-know), Vermeidung des Abflusses u.a. von Kontakt- Navigations-, Standorts- und Kommunikations(meta)daten, Vermeidung datenreicher Messenger (u.a. WhatsApp) und datenreicher sozialer Netzwerke (u.a. Facebook).[54]

1. dezentrale, Open-Source-basierte Netzwerke	Verwendung eines Netzwerks und Klienten aus dem Fediverse oder bereits existierende Schulnetzwerke die die Kommunikation über E-Mail mit eingeschalteter Verschlüsselung bereitstellen. Eine vorherige gezielte Prüfung ist anzuraten.[55]
2. Erkennen und Blockieren von Tracking	Verwendung u.a. von BLOCKADA für mobile Klienten und Privacy Badger für Webbrowser-basierte Dienste
3. Verwendung von datensparsamen Chat- und Messengerdiensten; Ver-schlüsselung	Sofern eine Lehrkraft es als notwendig erachtet, über Messenger mit Eltern, Schülerinnen und Schülern zu kommunizieren, kommen nur europäische Anbieter, die eine Ende-zu-Ende-Verschlüsselung anbieten, in Betracht, siehe z.B. Messenger auf dem Open Source-Kommunikationsprotokoll Jabber/XMPP oder auf E-Mail-Basis, z.B. Deltachat. Eine vorherige gezielte Prüfung ist anzuraten.
4. Einsatz alternativer Navigationsdienste	Vermeidung des Abflusses von Positionsdaten sowie Reiseplanungs- und Zieldaten durch Nutzung z.B. von: https://www.openstreetmap.org https://map.project-osrm.org https://maps.metager.de/map

Leitlinien für die Passwortwahl

Grundsatz: Passwörter sollten nur dem rechtmäßigen Besitzer bekannt sein und sich nicht durch Metawissen rekonstruieren/umgehen lassen, Passwörter sollten jeweils individuell für jeden Dienst/Account sein. Mögliche Bildungsvorschrift für sichere und merkfähige Passwörter: Bilden und Merken eines geheimen Satzes und Erzeugung des Passworts anhand z. B. der darin enthaltenen Anfangsbuchstaben und Zahlen.

[54] Siehe zum Beispiel https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Publikationen/flyer-schulischer-datenschutz.pdf und https://www.datenschutz.rlp.de/de/themenfelder-themen/datenschutz-in-der-schule-fragen-und-antworten-fuer-lehrkraefte/, Abrufdatum 3.9.2019.
[55] Siehe auch https://www.datenschutz.rlp.de/de/themenfelder-themen/datenschutz-in-der-schule-fragen-und-antworten-fuer-lehrkraefte/, Abrufdatum 3.9.2019.

1. Verwendung von sicheren Passwörtern	Passwortbildung mit mind. 10 Zeichen mit Sonderzeichen und Zahlen, Groß- und Kleinschreibung und ohne bekannte Wortbestandteile
2. Verwendung ausschließlich lokaler Passwortgeneratoren	Der Einsatz von Online-Passwortgeneratoren bzw. Managern verbietet sich automatisch aus der Zielstellung einer Geheimhaltung von Passwörtern.
3. Achtung bei Passwortsicherheitsabfragen	Passwortsicherheitsabfragen dienen bei vielen Online-Diensten dazu, Nutzer selbst dann zu identifizieren, wenn diese ihr Passwort vergessen haben. Oftmals sind die Sicherheitsabfragen auf vordefinierte Fragen beschränkt, in diesem Fall sind nur solche Fragen zu nutzen, deren Antwort durch Dritte nicht recherchierbar ist. Ist dies nicht möglich, sollten fiktive Antworten gegeben werden.

Leitlinien für E-Mail

Grundsatz: Einschränkung der Inhalte und des Leserkreises auf Adressaten und Absender, Minimierung der (Meta-)Datenspuren, Verhinderung von Bedrohungen der IT-Sicherheit durch E-Mails

1. Verwendung eines sicheren E-Mail Anbieters und Nutzung von Verschlüsselung	E-Mails sind ohne weitere Maßnahmen elektronische Postkarten, die von jedermann gelesen werden können. Deshalb wird die Verwendung eines bekannt sicheren E-Mail Anbieters notwendig. Schulen und Lehrkräfte können das Mailangebot des Landes für den dienstlichen Einsatz nutzen, persönliche Daten in Bezug auf einzelne Schülerinnen und Schüler sollten per Mail nicht unverschlüsselt versendet werden (z.B. Thunderbird mit Enigmail), bei der Nutzung des E-Maildienstes muss die Verbindungssicherheit (Verschlüsselung für das Login, Lesen und Senden) und die Benutzerauthentifzierung eingeschaltet sein.[56]
2. Verwendung von dedizierten externen E-Mail Programmen	Webmaildienste speichern und haben potentiell Zugriff auf Entwurfsfassungen von E-Mails und Kontaktadressen, deshalb Verwendung dedizierter, datensparsamer, Open-Source E-Mail-Programme wie z.B. Mozilla Thunderbird (Achtung, Konfiguration unter Datensparsamkeitsgesichtspunkten ist erforderlich.) Einbindung von Verschlüsselungsplugins wie Enigmail
3. Verwendung eines aktuellen Virenscanners	E-Mails können Schadcode enthalten. Ein Virenscanner mit aktuellem Datenstand ist deshalb Pflicht.
4. Plausibilitätsprüfung von E-Mails	Zur Vermeidung von (Spear-)Phishing-Angriffen sollten E-Mails immer in der Lang- oder Quellcodeansicht eingesehen werden. Dort enthaltene unbekannte Absender sollten als Warnsignal betrachtet werden.
5. Vermeidung von html-Mails und Nachladen von	In html-Mails können viele Kommandos und URL Aufrufe versteckt sein,

[56] Siehel https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Publikationen/flyer-schulischer-datenschutz.pdf.

Inhalten	deshalb die Ansicht generell auf Klartext (Plaintext) umstellen, ein Nachladen von Medien- und anderen Daten durch den E-Mail-Klienten sollte unterbunden werden.
6. Öffnen von Links im Webbrowser nach manueller Inspektion im URL-Feld	In E-Mails enthaltene Links sollten in die Adresszeile des Webbrowsers kopiert werden und mit denselben Vorsichtsmaßnahmen dort eingesehen werden wie bei allen anderen Browsingaktivitäten.
7. Verwendung von dienstlicher Mail und Verzicht auf Weiterleitung	Falls ein dienstliches E-Mail-Konto zur Verfügung steht, sollte dieses ausschließlich verwendet werden, wenn dienstliche Belange kommuniziert werden. Auf Weiterleitung auf andere E-Mail Konten ist zu verzichten.
8. Verschlüsselung	Verschlüsselung aller vertraulichen E-Mails z.B. mit GPG4Win für Windows bzw. KMail für Linux

Leitlinien für den Schulwebauftritt

Grundsatz: Schließen Sie Tracking durch Dritte aus. Nutzen Sie lokale Ansätze und den Schulhomepagebaukasten, den der Bildungsserver Sachsen-Anhalt zur Verfügung stellt.[57]

1. GoogleFonts und Webfonts	Tracking durch Fontsanbieter ausschließen durch lokale Nutzung der Fonts direkt auf dem genutzten Server oder Landesserver
2. Analytics	Falls die Nutzung von Analytics des Webauftritts dringend notwendig ist, muss der Zweck klar definiert und zweckgebunden sein. Im Sinne der Datenminimierung sollte Analytics lokal realisiert werden (z.B. via piwik/Matomo). Um Tracking durch Dritte auszuschließen, muss eine Reduktion der erfassten Daten auf das notwendige Minimum reduziert und Löschfristen angeben werden. Oftmals bieten Website-Tools bzw. Webseitenerstellungssoftware voreingestelltes Analytics, Trackings oder Drittanbietereinbindung (Fonts, Scripts, etc.). Hier muss darauf geachtet werden, dass diese nicht aktiv sind bzw. deaktiviert werden. Vor dem Hintergrund des besonderen Schutzbedarfs für Kinder ist GoogleAnalytics nicht zu empfehlen, da bei jedem Aufruf der Webseite der Verbindungsaufbau beim Drittanbieter sichtbar ist und im Allgemeinen protokolliert wird sowie die Daten zum Drittanbieter an Google (USA) übermittelt werden, auch wenn zuvor Anpassungen wie IP-Anonymisierungen erfolgten. Bei Nutzung der IP-Anonymisierung und opt-in statt opt-out muss die Zustimmung von Google AGBs erfolgen, um opt-out zu realisieren, Zwangszustimmung zum opt-out kann keine Lösung sein bzw. ist auf Schulrechnern von den Eltern selbst kaum zu realisieren oder vom Schüler selbst

[57] Siehe dazu https://www.bildung-lsa.de/medienberatung/schul_homepage_baukasten.html, Abrufdatum 30.07.2019.

	kaum realistisch zu organisieren,(siehe auch Diskussionen und Beschwerde in i). Google Analytics bietet Link-Attributation, was auch die individuellen Klicks protokollieren lässt (siehe FragFinn.de), was ebenfalls zur Individualisierung von Nutzern genutzt werden kann und ist vor dem Hintergrund des besonderen Schutzes von Kindern als ungeeignet einzuschätzen.
3. Einbinden von Videos	Videos direkt vom genutzten Server oder vom Bildungsserver Sachsen-Anhalt nutzen, um Tracking durch Dritte (z.B. Hoster wie YouTube/Akamai) auszuschließen
4. Karten- und Navigationsdienste	Nutzung datensparsamer Alternativen wie OpenStreetMap, OSRM oder Maps.Metager.de (https://www.openstreetmap.org/ https://map.project-osrm.org/, https://maps.metager.de/map)
5. Vorlesewerkzeuge	Verbindungsaufbau zeigt Nutzeraktivitäten: Nicht empfohlen werden Dienste außerhalb der EU, z.B. https://www.readspeaker.com/ - deshalb: Nutzung von datensparsamen, lokalen bzw. Landesserver-Diensten
6. Übersetzungswerkzeuge	Verbindungsaufbau zeigt Nutzeraktivitäten: Übersetzungstext wird an den Anbieter gesendet, was zu Urheberrechtsverstößen führen kann und zu Vertraulichkeitsverlust führt. Deshalb möglichst lokale oder Landesserver-Angebote vorziehen statt Drittanbieter-Cloud oder Drittanbieter-Lösungen.
7. Web-Baukästen	Bei der Verwendung von Werkzeugen oder Software-Baukästen bei der Webseitengestaltung werden oftmals Drittdiensteanbieter per Voreinstellung eingebunden (z.B. Analytics, Fonts, Karten- und Navigationsdienste, Vorlesdienste, Captchas usw.). Hier sollte eine Einschränkung auf lokale Dienste erfolgen oder Drittdienste gezielt ausgeschaltet werden.
8. Captchas	Mensch-Detektion wird oftmals als Baukasten realisiert und mit Drittanbieterdiensten verbunden, legt Nutzeraktivitäten offen. Die Nutzung von datensparsamen Diensten ist angezeigt. Captchas sind lokal oder mittels Landesserver umzusetzen, wie die lokale Variante von https://www.phpcaptcha.org/ (Achtung nur mit no-script ansurfen, Drittanbieter integriert).
9. Opt-In statt Opt-Out	Bei Privacy-relevanten Wahlmöglichkeiten soll prinzipiell die datensparsamste Einstellung als Vorgabe gewählt werden und der Nutzer dann umfassend auf Folgen anderer möglicher Wahlmöglichkeiten informiert werden (Opt-In). Während dieser Auswahl dürfen keine Daten bis zum Ende der Nutzerauswahl erfasst und übermittelt werden.
10. Terminplaner	Terminplaner können eine große Anzahl von Metadaten zusätzlich zum eigentlichen Eintrag vom Besucher erheben. Deshalb sollten bekannt datensparsame Alternativen genutzt werden, z.B. https://www.fdm.uni-hamburg.de/service/werkzeuge.html (Abrufdatum 30.07.2019).
11. Test des Webauftritts	Empfehlung: Automatisierte Tests können wichtige Bestandteile der IT-Sicherheits- und datenschutzrelevanten Umsetzung des Webauftritts automatisiert testen, z.B. mithilfe von

	https://privacyscore.org, https://webbkoll.dataskydd.net/de/, https://www.ssllabs.com/ssltest. Eine Verwendung sicherer Protokolle (https) für geschützte Bereiche und die explizite Kommunikation der offiziellen Webseite (URL) in Anschreiben/Mails ist notwendig.
12. Schulische Kommunikation zwischen Lehrkräften und Schülerinnen und Schülern	Zur schulischen Kommunikation zwischen Lehrkräften und Schülerinnen und Schülern steht den Schulen u.a. eine landeseigene, kostenfreie, auf Moodle basierende Lernplattform zur Verfügung. In der schulischen Kommunikation ist die Nutzung von datensparsamen, schullokalen oder landesweiten Diensten anzustreben.[58]

[58] Siehe auch https://www.datenschutz.rlp.de/de/themenfelder-themen/datenschutz-in-der-schule-fragen-und-antworten-fuer-lehrkraefte/, Abrufdatum 3.9.2019.

Anlage B Hardware

Die nachfolgenden Spezifikationen der beschriebenen Hardware-Komponenten sind eine Orientierung für die Beschaffung. Sie ersetzen im Einzelfall jedoch keine Ausschreibung, da dabei auch das Vergaberecht zu berücksichtigen ist. Die in den folgenden Tabellen als „Mindestkriterien“ bezeichneten Zeilen enthalten Informationen, die als technische Mindestanforderungen für die jeweilige IT-Geräteklasse zu verstehen sind. Darüber hinausgehende Beschreibungen dienen der weiterführenden Information und haben empfehlenden Charakter.[59]

Arbeitsplatzcomputer

Dieser Standard-PC eignet sich zum generellen Einsatz in der Schule. Bei speziellen Anwendungen (z. B. Videoschnittsoftware, CNC, 3D-CAD) können höhere Anforderungen notwendig sein, die in der Regel vom Hersteller spezifiziert werden. Nachfolgend ist ein Standardcomputer für die Betriebssysteme Windows, Linux oder MacOS beschrieben. Generell ist in Klassenräumen die Verwendung von Desktop-PC Geräten mit fester Verkabelung auch für das Netzwerk vorzuziehen (Lehrer- und Schülerarbeitsplatz). Hierdurch lässt sich die in der Bildschirmarbeitsplatzverordnung geforderte Ergonomie durch individuell einstellbare Geräte wie Tastatur und Bildschirm bestmöglich umsetzen. Die Bildschirmarbeitsplatzverordnung fordert sogar ausdrücklich eine Trennung von Bildschirm und Tastatur.[60]

Geräte ohne vorinstalliertes Betriebssystem/Applikationen bieten u.a. den Vorteil, zwischen verschiedenen Betriebssystemen wechseln bzw. um zukünftig bei gestiegenen Systemanforderungen eines Betriebssystems auf ressourcensparende Alternativen umsteigen zu können.

Datenblatt Arbeitsplatzcomputer		
Mindestkriterien: Werte für Systemleistung/CPU, RAM, Festplatte, Garantie		
Merkmal	Erläuterung / Hinweise	Werte
Systemleistung/ CPU	Um die Systemleistung zu überprüfen, eignet sich das Programm SYSmark 2014 oder das kostenlose Programm Cinebench R15. Bei aktuellen Komponenten kann davon ausgegangen werden, dass die geforderte Systemleistung bei folgenden Prozessoren erfüllt ist: ab Intel Pentium Gold G4560 ab Intel i3-6xxx ab Intel i5-6xxx ab Intel i7-6xxx ab AMD Ryzen 3 13xxx ab AMD Ryzen 5 xxxxx ab AMD Ryzen 7 xxxxx	Mindestwerte Benchmark: SYSmark 2014 v1.5 (Windows 10, 64bit): 1200 Punkte oder Cinebench R15: 145 Punkte (Single-Core) und 370 Punkte (Multi-Core)

[59] Sie orientieren sich an www.mebis.bayern.de/infoportal/empfehlung/votum/, Abrufdatum 19.9.2019.
[60] Bildschirmarbeitsverordnung: www.arbeitsschutzgesetz.org/bildscharbv/, Abrufdatum: 19.9.2019.

BIOS/UEFI	Manche Deploymentlösungen setzen einen Start im Legacy BIOS Modus voraus.	UEFI Modus und Legacy BIOS Modus
RAM	Um flüssiges Arbeiten zu ermöglichen, ist ausreichend Arbeitsspeicher erforderlich. Eine Erweiterung des Arbeitsspeichers (ohne Ausbau der vorhandenen Module) sollte möglich sein.	ab 8 GB RAM
Festplatte	Insbesondere beim Boot-Vorgang ist der schnelle Zugriff auf Daten gefordert. Daher empfiehlt sich der Einsatz einer Solid-State-Disk (SSD). Die typischen Transferraten liegen bei einer Anbindung über SATA III bei ca. 550 MB/s. Bei einem Anschluss über PCIe 3.0 x4 (M.2) sind höhere Transferraten möglich.	SSD: ab 240 GB
Grafik- /Sound- Anschlüsse	Grafik- und Soundanschlüsse sind meist auf dem Motherboard integriert, nur bei höheren Grafikanforderungen ist eine eigene Grafikkarte notwendig. Üblich sind mindestens ein digitaler Videoanschluss (HDMI) und Audio- Anschlüsse (Line in/out). Soll der PC zusätzlich an einen Beamer angeschlossen werden, ist ein weiterer kombinierter Audio-/Video- Ausgang sinnvoll (z. B. Zusatzkarte mit HDMI oder Display-Port).	frontseitige Audioanschlüsse für Kopfhörer/Mikrofon HDMI-Anschluss ggf. zusätzlich: weiterer HDMI-Anschluss oder Display-Port
USB-Anschlüsse	Sinnvoll sind mind. 4 USB- Anschlüsse, davon zwei leicht zugänglich an der Frontseite. USB 2.0 (bis 60 MByte/s) USB 3.0 (bis 500 MByte/s) USB 3.1 (bis 1200 MByte/s)	2 x USB 3.0 2 x USB 2.0 evtl. 1 x USB-C zwei USB-Anschlüsse an der Frontseite
LAN-Anschluss	Üblich ist ein RJ45-LAN-Anschluss für Gigabit-Ethernet mit Autosensing.	RJ45-LAN-Anschluss (Gigabit-Ethernet)
Optisches Laufwerk	Gegebenenfalls ist es sinnvoll, einzelne Rechner (z. B. Lehrer-PC) mit einem optischen Laufwerk auszustatten (DVD-Brenner oder Blu-ray-Brenner).	
Betriebssystem	Datensparsamkeit beachten und Verwendung freier Software - bzw. datensparsame Konfiguration	z.B. Linuxmuster – Windows 10 Education Pro oder Professional Versionen 64bit[61]
Geräuschentwicklung	Insbesondere in Computerräumen ist auf möglichst geräuscharme Systeme zu achten (Netzteil, Lüfter).	bis zu 26 dB bei 50% Last bis zu 20 dB bei Büroanwendungen

[61] Siehe dazu die Hinweis in: https://lfd.niedersachsen.de/download/144339, Abrufdatum: 17.09.2019.

Formfaktor, Gehäuse	Die unterschiedlichen Gehäusegrößen und -formen sind nicht exakt definiert. Verwendet werden die Begriffe Micro-PC, Mini- PC, Small-Form-Factor, All-in-One-PC. Je nach Einsatzort kann die maximale Größe festgelegt werden.	
Ergonomie, Zertifizierung	„Energy Star“ beschreibt Mindestanforderungen für die Energieeffizienz. „Blauer Engel“ ist ein Umweltprüfzeichen mit Kriterien zu Energieverbrauch, Materialanforderungen, Recyclingfähigkeit und Geräuschemission. Es gibt weitere Zertifizierungen, die gegebenenfalls gefordert werden können, aber nicht immer ausgewiesen sind, z.B. TCO Certified Desktops 5 oder energieeffizientes Netzteil nach „80 Plus Silver“.	
Garantie	gesetzlich garantiert sind 12 Monate Optional kann zur Sicherstellung der für den Nutzer erforderlichen Wiederherstellungszeiten ein separater EVB-IT Vertrag abgeschlossen werden (innerhalb der gesetzlichen Garantiezeit und auch darüber hinaus).	Laufzeit EVB-IT Vertrag 1-5 Jahre Empfehlung: 3 Jahre
Beschaffung	ggf. Aufstellen und Anschließen der PCs, umweltgerechte Entsorgung der Verpackungen	

Monitor

Datenblatt Monitor		
Mindestkriterien: Werte für Größe, Auflösung, Helligkeit		
Merkmal	Erläuterung / Hinweise	Werte
Größe	Bildschirmdiagonalen von 24" sind Standard. Für die Bildbearbeitung sind größere Monitore mit einer entsprechend höheren Auflösung empfehlenswert.	ab 23,5"
Panel	Von den derzeit verfügbaren Panel- Technologien bieten IPS-Panels das beste Bild und den größten Blickwinkel.	IPS-Panel
Auflösung		bis 24" Bildschirm: ab 1920 x 1080 Pixel bzw. ab 1920 x 1200 Pixel bei Bildschirmen > 24":
Helligkeit	Da in Klassenzimmern und Computerräumen an verschiedenen Arbeitsplätzen unterschiedliche Lichtverhältnisse herrschen, sollte der Monitor hell genug sein und ein gutes Kontrastverhältnis für die Darstellung von satten Farben und einen gut lesbaren Text haben.	ab 300 cd/m²
Reaktionszeit	Eine niedrige Reaktionszeit (grau zu grau) ist für die flüssige Darstellung von bewegten Inhalten notwendig.	max. 5 ms
Anschlüsse	Neben digitalen Eingängen sollte zum Anschluss älterer Rechner auch ein VGA-Anschluss vorhanden sein.	HDMI oder DisplayPort VGA
Ergonomie	Der Monitor sollte in der Höhe und Neigung verstellbar sein.	Stabiler Standfuß, höhenverstellbar, neigbar

Zertifizierung	„Blauer Engel“ ist ein Umweltprüfzeichen mit Kriterien zu Energieverbrauch, Materialanforderungen, Recyclingfähigkeit und Geräuschemission. TCO Certified Displays ist ein Gütesiegel für Bildschirme, das u. a. ergonomische Kriterien (Helligkeit, Kontrast, Sehwinkel, reflexionsfreie Oberfläche) und auch die Anforderungen des „Energy Star“ beinhaltet. Zunehmend wird auch bei Monitoren ein EU-Energielabel ausgewiesen (z. B. EU-Energielabel A+).	Blauer Engel (RAL-UZ 78c für Monitore) TCO Certified Displays 7
Zusatzoptionen	integrierte Lautsprecher, Kopfhörer- und Mikrophon-Anschlüsse, USB- Anschlüsse	
Garantie	Da aktuelle Monitore relativ günstig und haltbar sind, ist eine erweiterte Garantie nicht notwendig.	gesetzliche Gewährleistung

Notebook

Die Auswahl richtet sich nach den Mobilitätsanforderungen (Ersatz für einen Desktop- Computer oder mobiles Gerät) und der erforderlichen Ausstattung (z.B. DVD- Laufwerk, Schnittstellen). Nachfolgend ist ein Notebook für die Betriebssysteme Windows, Linux oder MacOS beschrieben. Geräte ohne vorinstalliertes Betriebssystem/Applikationen bieten u.a. den Vorteil, zwischen verschiedenen Betriebssystemen wechseln bzw. um zukünftig bei gestiegenen Systemanforderungen eines Betriebssystems auf ressourcensparende Alternativen umsteigen zu können. Bei Notebooks ist auf die sichere Verwahrung besonders zu achten und die Möglichkeit, die zentrale Ladung der Akkus zu ermöglichen.

Datenblatt Notebook		
Mindestkriterien: Werte für Systemleistung/CPU, RAM, Festplatte, Display, Garantie		
Merkmal	Erläuterung / Hinweise	Werte
Systemleistung/ CPU	Um die Systemleistung zu überprüfen, eignet sich das Programm SYSmark 2014 oder das kostenlose Programm Cinebench R15. Typischerweise werden die Bench- markwerte nur erreicht, wenn das Notebook an eine externe Stromquelle angeschlossen ist und nicht übermäßig erhitzt ist. Bei aktuellen Komponenten kann davon ausgegangen werden, dass die gefor-derte Systemleistung bei folgenden Prozessoren erfüllt ist: ab Intel i5-73xxU / ab Intel i7-7xxxx / ab AMD Ryzen 7 3700U	Mindestwerte Benchmark: SYSmark 2014 v1.5 (Windows 10, 64bit): 1200 Punkte oder Cinebench R15: 145 Punkte (Single-Core) und 370 Punkte (Multi-Core)
BIOS/UEFI	Manche Deploymentlösungen setzen einen Start im Legacy BIOS Modus voraus.	UEFI Modus und Legacy BIOS Modus
RAM	Um flüssiges Arbeiten zu ermöglichen, ist ausreichend Arbeitsspeicher erforderlich.	ab 8 GB RAM
Festplatte	Insbesondere beim Boot-Vorgang ist der schnelle Zugriff auf Daten gefordert. Daher empfiehlt sich der Einsatz einer Solid-State-Disk (SSD).	SSD: ab 128 GB
Display	Empfohlen wird ein mattes Display (non-glare), da dieses Reflexionen vermeidet und somit ein angenehmeres Arbeiten ermöglicht. Bei Notebooks, die über einen Touchsscreen verfügen (z.B. Convertibles), sind matte Displays dagegen kaum verfügbar.	ab 1920 x 1080 Pixel

Grafik- / Sound- Anschlüsse	Zum Anschluss an einen Beamer oder externen Monitor ist ein Grafikanschluss notwendig. Üblich ist ein digitaler Anschluss (Display-Port, Mini-Display-Port, HDMI, Mini-HDMI, USB-C). Ggf. sind Adapter notwendig.	Display-Port, Mini-Display-Port, USB-C oder HDMI Kopfhörer/Mikrofon-Anschluss
USB-Anschlüsse	Sinnvoll sind mind. 2 USB-Anschlüsse. USB 2.0 (bis 60 MByte/s) USB 3.0 (bis 500 MByte/s) USB 3.1 (bis 1200 MByte/s)	USB 3., 1 x USB-C
LAN-Anschluss	Bei kleineren Notebooks ist der LAN-An-schluss nur über einen Adapter (z.B. USB-C auf RJ45-Adapter) möglich.	
WLAN		802.11ac
Betriebssystem	Datensparsamkeit beachten und Verwendung freier Software - bzw. datensparsame Konfiguration	z.B. Linuxmuster – Windows 10 Education Pro oder Professional Versionen 64bit[62]
weitere optionale Ausstattungen	integriertes Blu-ray oder DVD-Laufwerk / Brenner integrierte Lautsprecher Kartenlesegerät eingebaute Kamera Fingerprint-Sensor Kensington-Schutz Docking-Anschluss	
Ergonomie, Zertifizierung	„Energy Star“ beschreibt Mindestanforderungen für die Energieeffizienz. Weitere Zertifizierungen sind bei Notebooks meist nicht ausgewiesen. Da Notebooks ggf. mechanisch stark beansprucht werden, sollte man auf robuste Geräte achten. Dies gilt z.B. für Geräte, die nach dem MIL-STD-810G zertifiziert sind.	
Garantie	Gesetzlich garantiert sind 12 Monate. Optional kann zur Sicherstellung der für den Nutzer erforderlichen Wiederherstellungszeiten ein separater EVB-IT Vertrag abgeschlossen werden (innerhalb der gesetzlichen Garantiezeit und auch darüber hinaus).	Laufzeit EVB-IT Vertrag 1-5 Jahre Empfehlung: 3 Jahre

[62] Siehe dazu die Hinweis in: https://lfd.niedersachsen.de/download/144339, Abrufdatum: 17.09.2019.

Tablets

Bei der Auswahl eines Tablets stehen das Betriebssystem und die damit verbundenen Anwendungen im Vordergrund. Bei schuleigenen Tablets wird zur einfacheren Administration ein Mobile Device Management-System (MDM-System) empfohlen.
Die Fingerbedienung eines Tablets wird durch eine kapazitive Technologie erkannt. Soll ein Tablet auch zum Schreiben (digitale Heftführung oder als Whiteboardersatz) geeignet sein, ist eine präzise Stifteingabe notwendig. Induktive Stifte (aktive Stifte) ermöglichen dies und unterstützen mehrere Druckstufen. Durch die Unterscheidung zwischen kapazitiver Berührung und induktivem Stift ist auch eine Handballenerkennung möglich. Bei Tablets ist auf die sichere Verwahrung besonders zu achten und die Möglichkeit, die zentrale Ladung der Akkus zu ermöglichen. Geräte ohne vorinstalliertes Betriebssystem/Applikationen bieten u.a. den Vorteil, zwischen verschiedenen Betriebssystemen wechseln bzw. um zukünftig bei gestiegenen Systemanforderungen eines Betriebssystems auf ressourcensparende Alternativen umsteigen zu können. Bei Tablets ist auf die sichere Verwahrung besonders zu achten und die Möglichkeit, die zentrale Ladung der Akkus zu ermöglichen.

Datenblatt PC-Tablet		
Mindestkriterien: Werte für Systemleistung/CPU, RAM, interner Speicher, Display		
Merkmal	Erläuterung / Hinweise	Werte
Systemleistung/ CPU	Um die Systemleistung zu überprüfen, eignet sich das kostenlose Programm Cinebench R15. Typischerweise werden die Benchmarkwerte nur erreicht, wenn das Tablet an eine externe Stromquelle angeschlossen ist und nicht übermäßig erhitzt ist. Bei aktuellen Komponenten kann davon ausgegangen werden, dass die geforderte Systemleistung bei folgenden Prozessoren erfüllt ist: ab Intel Celeron N4xx ab Intel Pentium Silver N5xx ab Intel Pentium Gold 4xxx Intel Core m-5xxxx ab Intel Core m3-xxxx ab Intel i3-6xxxU ab Intel i5-6xxxU ab Intel i7-6xxxx	Mindestwerte Benchmark: Cinebench R15: 60 Punkte (Single-Core) und 150 Punkte (Multi-Core)
RAM		ab 4 GB RAM
interner Speicher		SSD ab 64 GB
Display	Gefordert wird ein blickwinkelstabiles Display mit einem Touchscreen und einem Digitizer oder einer vergleichbaren Technik zur Stifteingabe mit mehreren Druckstufen und einer zuverlässigen Handballenerkennung.	ab 9,5" Bildschirmdiagonale mind. 2 MegaPixel Digitizer (Stifteingabe mit mehreren Druckstufen)

Grafik-/Sound-Anschlüsse	Zum Anschluss an einen Beamer oder externen Monitor ist ein Grafikanschluss notwendig. Üblich ist ein digitaler Anschluss (Display-Port, Mini-Display-Port, HDMI, Mini-HDMI). Ggf. sind Adapter, z.B. USB-C, notwendig.	Display-Port, Mini-Display- Port oder HDMI, ggf. via USB-C
WLAN		802.11ac
Betriebssystem	Datensparsamkeit beachten und Verwendung freier Software - bzw. datensparsame Konfiguration	z.B. Linuxmuster – Windows 10 Education Pro oder Professional Versionen 64bit[63]
Gewicht		bei 10": max 800 g, bei 12": max 1000 g
Sonstiges	Ein Gyroskop ist für AR- und VR- Anwendungen notwendig. Auf eine möglichst lange Akkulaufzeit sollte geachtet werden. Da Tablets ggf. mechanisch stark beansprucht werden, sollte man auf robuste Geräte achten.	
Garantie	gesetzlich garantiert sind 12 Monate Optional kann zur Sicherstellung der für den Nutzer erforderlichen Wiederherstellungszeiten ein separater EVB-IT Vertrag abgeschlossen werden (innerhalb der gesetzlichen Garantiezeit und auch darüber hinaus).	Laufzeit EVB-IT Vertrag 1-5 Jahre Empfehlung: 3 Jahre

[63] Siehe dazu die Hinweis in: https://lfd.niedersachsen.de/download/144339, Abrufdatum: 17.09.2019.

Datenblatt Android- bzw. ChromeOS-Tablet[64]		
Mindestkriterien: Werte für Systemleistung/CPU, RAM, interner Speicher, Display		
Merkmal	Erläuterung / Hinweise	Werte
Systemleistung/ CPU	Um die Systemleistung zu überprüfen, eignen sich die kostenlosen Programme AnTuTu oder Geek-Bench. Bei aktuellen Komponenten kann davon ausgegangen werden, dass die geforderte Systemleistung bei folgenden Prozessoren erfüllt ist: RK3399 MT8163 Helio ab X20 Kirin 659, 950, 960 Snapdragon ab 625	Mindestwerte Benchmark: AnTuTu v7-Benchmark: 75.000 Punkte (Total Score) oder GeekBench 4 900 Punkte (Single-Core) und 3500 Punkte (Multi-Core)
RAM		ab 2 GB RAM
interner Speicher	Eine Möglichkeit zur Erweiterung des internen Speichers mit einer Speicherkarte ist meist gegeben.	ab 32 GB
Display	Gefordert wird ein blickwinkelstabiles Display mit einem Touchscreen und einem Digitizer oder einer vergleichbaren Technik zur Stifteingabe mit mehreren Druckstufen und einer zuverlässigen Handballenerkennung.	ab 10" Bildschirmdiagonale mind. 2 MegaPixel Digitizer (Stifteingabe mit mehreren Druckstufen)
Grafik- / Sound- Anschlüsse	Zum Anschluss an einen Beamer oder externen Monitor ist ein Grafikanschluss notwendig. Üblich ist ein digitaler Anschluss (Display-Port, Mini-Display-Port, HDMI, Mini-HDMI). Ggf. sind Adapter, z.B. USB-C, notwendig.	Display-Port, Mini-Display- Port oder HDMI, ggf. via USB-C
WLAN		802.11ac

[64] Bei der Benutzung von ChromeBooks mit ChromeOS entstehen zwangsläufig Verbindungen zu Clouddiensten. Cloudbasierte Produkte sind datenschutzrechtlich anspruchsvoll (siehe Abschnitt 6.2 und www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Publikationen/flyer-schulischer-datenschutz.pdf), Abrufdatum: 19.09.2019).

Betriebssystem/ Software	Für die Updates des Betriebssystems ist der Gerätehersteller zuständig. Daher sollten Hersteller gewählt werden, die System-Updates auch für ältere Geräte liefern. Fokus auf Datensparsamkeit und Verwendung freier Software – bzw. datensparsame Konfiguration	ab Android 9 bzw. aktuelles Chrome OS
Gewicht		bei 10": max 600 g, bei 12": max 800 g
Sonstiges	Ein Gyroskop ist für AR- und VR- Anwendungen notwendig. Auf eine möglichst lange Akkulaufzeit sollte geachtet werden. Da Tablets ggf. mechanisch stark beansprucht werden, sollte man auf robuste Geräte achten.	
Garantie	Gesetzlich garantiert sind 12 Monate. Optional kann zur Sicherstellung der für den Nutzer erforderlichen Wiederherstellungszeiten ein separater EVB-IT Vertrag abgeschlossen werden (innerhalb der gesetzlichen Garantiezeit und auch darüber hinaus).	Laufzeit EVB-IT Vertrag 1-5 Jahre Empfehlung: 3 Jahre

Datenblatt iOS-Tablet		
Mindestkriterien: Werte für Systemleistung/CPU, RAM, interner Speicher, Display		
Merkmal	Erläuterung / Hinweise	Werte
Systemleistung/ CPU	Um die Systemleistung zu überprüfen, eignet sich das Programm AnTuTu. Aktuelle iPads (ab Apple A10- Prozessor) erfüllen die geforderte Systemleistung.	Mindestwerte Benchmark: AnTuTu v7-Benchmark: 200.000 Punkte (Total Score)
RAM		ab 2 GB RAM
interner Speicher	Wenn viele Apps installiert werden oder wenn das iPad für Video- Aufnahmen genutzt wird, ist mehr Speicher erforderlich.	ab 32 GB
Display	Alle aktuellen iPads bieten ein blickwinkelstabiles Display mit der Möglichkeit der Stifteingabe mit mehreren Druckstufen und einer zuverlässigen Handballenerkennung.	ab 9,5" Bildschirmdiagonale mind. 2 MegaPixel Digitizer (Stifteingabe mit mehreren Druckstufen)
Grafik- / Sound- Anschlüsse	Zum Anschluss an einen Beamer oder externen Monitor ist ein Grafikanschluss notwendig. Üblich ist ein digitaler Anschluss (Display-Port, Mini-Display-Port, HDMI, Mini-HDMI). Ggf. sind Adapter, z.B. USB-C/Lightning, notwendig.	Display-Port, Mini-Display-Port oder HDMI, ggf. via USB-C/Lightning
WLAN		802.11ac
Betriebssystem/ Software	Beachtung von Datensparsamkeit und Verwendung freier Software, datensparsame Konfiguration.[65] Die Installation von Apps erfolgt über den Apple App-Store. Drucken ist über Air-Print möglich.	aktuelles iOS
Gewicht		bei 10": max 600 g bei 12": max 800 g

[65] Siehe dazu www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Publikationen/flyer-schulischer-datenschutz.pdf, Abrufdatum: 19.09.2019.

Sonstiges	Alle aktuellen iPads enthalten ein Gyroskop (für AR- und VR- Anwendungen) und verfügen über eine lange Akkulaufzeit. Ein Hardcover zum Schutz der Geräte vor leichten Stößen ist empfehlenswert. Da Tablets ggf. mechanisch stark beansprucht werden, sollte man auf robuste Geräte achten.	
Garantie	Gesetzlich garantiert sind 12 Monate. Optional kann zur Sicherstellung der für den Nutzer erforderlichen Wiederherstellungszeiten ein separater EVB-IT Vertrag abgeschlossen werden (innerhalb der gesetzlichen Garantiezeit und auch darüber hinaus).	Laufzeit EVB-IT Vertrag 1-5 Jahre Empfehlung: 3 Jahre

Server

Server sollten differenziert nach dem jeweiligen Einsatzbereich ausgewählt werden. Nachfolgend sind je ein Standardserver und ein Server zur Virtualisierung von Serversystemen spezifiziert.

Datenblatt Standardserver (z. B. Fileserver ohne Virtualisierung von Serversystemen)		
Werte für Systemleistung/CPU, RAM, LAN-Anschlüsse, Garantie		
Merkmal	Erläuterung / Hinweise	Werte
Systemleistung/ CPU	Um die Prozessorleistung zu überprüfen, eignet sich der Benchmark SPEC CPU 2006[66] Bei aktuellen Komponenten kann davon ausgegangen werden, dass die geforderte Systemleistung bei folgenden Prozessoren erfüllt ist: ab Intel Xeon E3-1220 v6 ab Intel Xeon Bronze	mind. 4-Kern-CPU Benchmark SPEC-CPU-2006 SPECint_rate_base 2006: ab 200
RAM	Bei der Belegung der Steckplätze mit RAM-Modulen sollten die Herstellervorgaben bez. der Aufteilung auf die Speicherkanäle beachtet werden, um Leistungseinbußen zu vermeiden. Für eine spätere Erweiterungsmöglichkeit sollten noch Steckplätze zur Verfügung stehen. ECC-Arbeitsspeicher beinhalten eine Fehlerkorrektur, die für Server im Dauerbetrieb sinnvoll ist.	ab 16 GB RAM ab DDR 4 ECC 2133 MT/s
Festplatte (HDD)	Wichtig ist, dass Server-Festplatten für den Dauer-Einsatz verwendet werden. Ggf. können auch zwei Festplatten (für System und Daten) sinnvoll sein.	HDD: 1 x 2 TB

[66] Siehe www.spec.org/cgi- bin/osgresults?conf=cpu2006 (CINT2006 Rates), Abrufdatum: 09.07.2019.

USB-Anschlüsse	Je nach vorgesehener Anwendung (z. B. Datensicherung mit mobilen USB-Festplatten), können auch USB- Anschlüsse an der Frontseite sinnvoll sein.	ab 4 x USB 3.0
LAN-Anschlüsse		2 x RJ45-LAN (Gigabit-Ethernet)
Betriebssystem	Datensparsamkeit beachten und Verwendung freier Software - bzw. datensparsame Konfiguration	z.B. Linuxmuster – Windows 10 Education Pro oder Professional Versionen 64bit[67]
Geräuschentwicklung	Falls der Server in einem Raum steht, in dem sich gelegentlich Personen aufhalten, ist auf geräuscharme Systeme zu achten (Netzteil, Lüfter).	
Formfaktor, Gehäuse	Üblich sind Tower oder 19"-Gehäuse zum Einbau in ein Rack.	Tower
Garantie	Gesetzlich garantiert sind 12 Monate. Optional kann zur Sicherstellung der für den Nutzer erforderlichen Wiederherstellungszeiten ein separater EVB-IT Vertrag abgeschlossen werden (innerhalb der gesetzlichen Garantiezeit und auch darüber hinaus).	Laufzeit EVB-IT Vertrag 1-5 Jahre Empfehlung: 3 Jahre

[67] Siehe dazu die Hinweise in: https://lfd.niedersachsen.de/download/144339, Abrufdatum: 17.09.2019.

Datenblatt Server (zur Virtualisierung von Serversystemen)		
Werte für Systemleistung/CPU, RAM, LAN-Anschlüsse, Garantie		
Als Virtualisierungssystem wird primär VMware ESXi (kostenlose Version oder Essentials-Version) oder Microsoft Hyper-V eingesetzt. Die Hardware sollte so ausgelegt sein, dass mehrere Serversysteme virtualisiert werden können.		
Merkmal	Erläuterung / Hinweise	Werte
Systemleistung/ CPU	Um die Prozessorleistung zu überprüfen, eignet sich der Benchmark SPEC CPU 2006. Bei aktuellen Komponenten kann davon ausgegangen werden, dass die geforderte Systemleistung bei folgenden Prozessoren erfüllt ist: ab Intel Xeon E5-2630 v4 ab Intel Xeon Silver 4110 ab AMD Epyc 7351	mind. 8-Kern-CPU Benchmark SPEC-CPU-2006 SPECint_rate_base2006: ab 600
RAM	Bei der Belegung der Steckplätze mit RAM-Modulen sollten die Herstellervorgaben bez. der Aufteilung auf die Speicherkanäle beachtet werden, um Leistungseinbußen zu vermeiden. Für eine spätere Erweiterungsmöglichkeit sollten noch Steckplätze zur Verfügung stehen. ECC-Arbeitsspeicher beinhalten eine Fehlerkorrektur, die für Server im Dauerbetrieb sinnvoll ist.	ab 64 GB RAM ab 2400 MT/s ECC RDIMMs
SSD	Die Installation des Virtualisierungsservers (ESXi, Hyper-V) erfolgt vorzugsweise auf einem Flash- oder auf einem schnellen SSD-Speicher.	ESXi: 16 GB Flash Hyper-V: 128 GB SSD
HDD	Vier Festplatten im RAID-5-Verbund mit einem Hardware-Controller; ggf. Hot Spare	HDD: 4 x 2 TB SAS-Platten Controller: RAID 5
USB-Anschlüsse		4 x USB 3.0
LAN-Anschlüsse	Je nach vorgesehenem Einsatz sind 2-4 LAN-Anschlüsse sinnvoll (z. B: Link Aggregation, Anbindung eines externen Storage). Gegebenenfalls können auch 2 x 10 GBit/s-Ethernet-Anschlüsse sinnvoll sein.	4 x RJ45-LAN (Gigabit-Ethernet)

Betriebssystem	Datensparsamkeit beachten und Verwendung freier Software - bzw. datensparsame Konfiguration	z.B. Linuxmuster – Windows 10 Education Pro oder Professional Versionen 64bit[68]
Verwaltung	Zur Fernwartung des Servers über das Netzwerk kann eine Managementcard (Out of Band Management) sinnvoll sein.	Out of Band Management
Gehäuse		19"-Gehäuse
Stromversorgung		Redundantes Netzteil
Garantie	Gesetzlich garantiert sind 12 Monate. Optional kann zur Sicherstellung der für den Nutzer erforderlichen Wiederherstellungszeiten ein separater EVB-IT Vertrag abgeschlossen werden (innerhalb der gesetzlichen Garantiezeit und auch darüber hinaus).	Laufzeit EVB-IT Vertrag 1-5 Jahre Empfehlung: 3 Jahre

[68] Siehe dazu die Hinweise in: https://lfd.niedersachsen.de/download/144339, Abrufdatum: 17.09.2019.

NAS-Systeme

NAS-Systeme (Network Attached Storage) sind ursprünglich als Datenablagen konzipierte Speichersysteme mit großem Festplattenspeicherplatz, die direkt aus dem Netzwerk erreichbar sind. Mittlerweile bieten NAS-Systeme eine Vielzahl weiterer Zusatzdienste an (z. B. Backup-Server, einfacher Virtualisierungs-Server, Medienserver, Web-Server, SQL-Server, VPN-Server, Speicher für Videoüberwachung,[69] Cloud-Dienste). Die Lese- und Schreibrechte auf Freigaben können benutzerspezifisch geregelt werden, die Zugriffe sind mit unterschiedlichen Protokollen möglich, z. B. über smb, AppleTalk, ftp, http oder bei mobilen Geräten über Apps.
Aktuelle NAS-Systeme bieten auch die Möglichkeit, virtuelle Maschinen auf dem NAS- System zu betreiben. Diese Funktion ist jedoch eher für den Home-Bereich gedacht; die Virtualisierung von Serversystemen erfordert sehr viel Rechenleistung und ist bei den derzeitigen NAS-Systemen nur eingeschränkt möglich.

Datenblatt NAS-System für den Unterrichtsbetrieb		
Mindestkriterien: Werte für Systemleistung/CPU, RAM, LAN-Anschlüsse		
Merkmal	Erläuterung / Hinweise	Werte
Systemleistung/ CPU	Für viele Serverdienste oder gleichzeitige Zugriffe mehrerer Personen und eine kurze Reaktionszeit ist ein leistungsfähiger Prozessor erforderlich.	ab Quadcore-Prozessor (x86-Architektur) mit mind. 1,5 GHz Taktfrequenz
RAM	Für viele Serverdienste, gleichzeitige Zugriffe mehrerer Personen und eine hohe Schreib- und Lesegeschwindigkeit ist ausreichend Arbeitsspeicher erforderlich.	ab 2 GB RAM
Konfiguration	Die normale Konfiguration erfolgt über eine Weboberfläche. Der Zugriff auf das Dateisystem über SSH sollte möglich sein. Sinnvoll ist es, wenn die NAS-Box Systemmeldungen (Speicherplatz oder Festplattenfehler) per E-Mail verschickt.	Konfiguration über eine Weboberfläche (Webinterface auf Deutsch) Zugriffsmöglichkeit über SSH Benachrichtigung per E- Mail bei Systemwarnungen
Festplatteneinschübe	Sinnvoll sind NAS-Systeme mit mind. 4 Festplatteneinschüben (3,5").	4 Festplatteneinschübe mit 3,5"

[69] Siehe dazu das Kurzpapier zur Videoüberwachung unter www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html, Abrufdatum 18.9.2019

Festplatten (HDD)	Es sollten SATA-Festplatten verwendet werden, die für den Dauerbetrieb (Servereinsatz oder NAS-Einsatz, 24/7) geeignet sind. Ggf. kann es sinnvoll sein, eine weitere Festplatte (als Vorrat) zu beschaffen, damit im Falle eines Festplattendefekts entsprechend schnell reagiert werden kann.	4 SATA-Platten je 2 TB geeignet für den Dauerbetrieb (NAS-Festplatten) Hot-Swap-Fähigkeit; ggf. Hot-Spare-Festplatte
Controller	Hardware-Controller mit der Möglichkeit, unterschiedliche Raid- Level zu realisieren (z. B. RAID 1, RAID 5, RAID 6, ggf. Hotspare); Festplatten sollen im laufenden Betrieb gewechselt werden können.	Hardware-Controller mit RAID 5, RAID 6
LAN-Anschlüsse	Sinnvoll sind derzeit 2-4 RJ45-LAN- Anschlüsse mit Gigabit-Ethernet und der Möglichkeit der Link-Aggregation; ggf. Einschubmöglichkeit für 10 GBit/s-Netzwerkkarte	ab 2 x RJ45-LAN (Gigabit-Ethernet)
Leistung (Datendurchsatz, Verbindungen)	Bei 2 Netzwerkanschlüssen sollte der Datendurchsatz 200 MByte/s betragen (bei RAID 5, Windows Upload/Download), bei 4 Netzwerkkarten 400 MByte/s. Die Zahl der maximal gleichzeitigen Verbindungen sollte hoch genug sein.	200 MByte/s (Windows Upload/Download bei RAID 5) 500 gleichzeitige Verbindungen
USB-Anschlüsse	Sinnvoll sind mind. 2 USB-Anschlüsse mit USB 3.0 zum Anschluss eines Backup-Mediums.	2 x USB 3.0
Betriebssystem	Datensparsamkeit beachten und Verwendung freier Software - bzw. datensparsame Konfiguration	z.B. Linuxmuster – Windows 10 Education Pro oder Professional Versionen 64bit[70]
Benutzerverwaltung	Möglichkeit der lokalen Benutzerverwaltung, Gruppenverwaltung und ggf. Active-Directory-Authentifizierung (Benutzerverwaltung über einen Windows-Server) ggf. Quota-Regelung für Benutzer	2000 Benutzerkonten Quota-Regelung für die Benutzer
Zugriffsmöglichkeiten	Die Benutzer sollten auf das NAS mit gängigen Werkzeugen zugreifen können (Windows-Zugriffe bzw. SMB, AppleTalk, NFS, FTP, http). Für den Zugriff von mobilen Geräten sollte eine App verfügbar sein.	Zugriffe über SMB, AppleTalk, NFS, FTP, http App für mobile Geräte

[70] Siehe dazu die Hinweise in: https://lfd.niedersachsen.de/download/144339, Abrufdatum: 17.09.2019.

optionale Zusatzfunktionen	Je nach vorgesehenem Einsatz können Zusatzfunktionen von Interesse sein, die viele NAS- Systeme anbieten: Webserver: z.B. für schulinterne Webseiten, ggf. mit Zusatz-Apps (Moodle, Joomla) Datenbankserver: üblicherweise ein MySQL-Server, der aktiviert werden kann iSCSI-Speicher: z.B. als externer Speicher für Virtualsierungslösungen Verschlüsselung Virenscanner: mit automatisierten Updates und Suchfunktionen Automatisierte Backupfunktion (z.B. auf eine andere NAS oder eine angeschlossene Festplatte), ggf. auch mit One-Touch-Taste (Backup auf eine USB-Platte per Tastendruck) Medienserver Radius-Server	
weitere optionale Ausstattungen	Reset-Knopf (Passwort zurücksetzen) Kensington-Schutz HDMI-Anschluss	
Energieverbrauch	Üblich sind bis zu 50 W im Betrieb (mit 4 Festplatten) und bis zu 30 W im Standby (HDD-Ruhezustand). Bei einigen NAS-Systemen lässt sich ein Sleep-Modus einstellen (max. 1 W). Wenn das NAS im Sleep- Modus ist, dauert der erste Zugriff länger (Starten des Systems, Hochfahren der Festplatten).	max. 50 W (Betrieb) max. 30 W (Standby) max. 1 W (Sleep-Modus)
Geräuschentwicklung	Falls das NAS in einem Raum steht, in dem sich gelegentlich Personen aufhalten, ist auf geräuscharme Systeme zu achten (Netzteil, Lüfter). Leistungsstarke NAS-Systeme sind üblicherweise lauter.	max. 21 dB (im Betriebs- Modus, bei laufenden Festplatten)
Garantie	Gesetzlich garantiert sind 12 Monate. Optional kann zur Sicherstellung der für den Nutzer erforderlichen Wiederherstellungszeiten ein separater EVB-IT Vertrag abgeschlossen werden (innerhalb der gesetzlichen Garantiezeit und auch darüber hinaus).	Laufzeit EVB-IT Vertrag 1-5 Jahre Empfehlung: 3 Jahre

Datenblatt Einfaches NAS (z. B. zur Datensicherung)		
Mindestkriterien: Werte für Systemleistung/CPU, RAM, LAN-Anschlüsse		
Merkmal	Erläuterung / Hinweise Beschreibung	Werte
Systemleistung/ CPU	Für kleine Benutzergruppen (höchstens fünf gleichzeitige Zugriffe) oder als Backupsystem ist ein Embedded-Prozessor ausreichend.	ab Quadcore-Embedded- Prozessor mit mind. 1 GHz Taktfrequenz
RAM		ab 1 GB RAM
Konfiguration	Die normale Konfiguration erfolgt über eine Weboberfläche. Der Zugriff auf das Dateisystem über SSH sollte möglich sein. Sinnvoll ist es, wenn die NAS-Box Systemmeldungen (Speicherplatz oder Festplattenfehler) per E-Mail verschickt.	Konfiguration über eine Weboberfläche (Webinterface auf Deutsch) Zugriffsmöglichkeit über SSH Benachrichtigung per E- Mail bei Systemwarnungen
Festplatteneinschübe	Sinnvoll sind NAS-Systeme mit mind. 2 Festplatteneinschüben (3,5")	2 Festplatteneinschübe mit 3,5"
Festplatten (HDD)	Es sollten SATA-Festplatten verwendet werden, die für den Dauerbetrieb (Servereinsatz oder NAS-Einsatz, 24/7) geeignet sind. Ggf. ist es sinnvoll, eine weitere Festplatte (als Vorrat) zu beschaffen, damit im Falle eines Festplatten- defekts entsprechend schnell reagiert werden kann.	2 SATA-Platten je 2 TB geeignet für den Dauerbetrieb (NAS- Festplatten)
RAID-Level	JBOD, RAID 0/1	RAID 1
LAN-Anschlüsse	Standard ist derzeit ein RJ45-LAN- Anschluss mit Gigabit-Ethernet.	ab 1 x RJ45-LAN (Gigabit-Ethernet)
USB-Anschlüsse	Sinnvoll sind mind. 2 USB- Anschlüsse mit USB 3.0 zum Anschluss eines Backup-Mediums.	2 x USB 3.0
Benutzerverwaltung	Möglichkeit der lokalen Benutzer- verwaltung, Gruppenverwaltung	Mehrere Benutzerkonten
Zugriffsmöglichkeiten	Die Benutzer sollten auf das NAS mit gängigen Werkzeugen zugreifen können. Für den Zugriff von mobilen Geräten sollte eine App verfügbar sein.	Zugriffe über SMB, App für mobile Geräte

optionale Zusatzfunktionen	Je nach vorgesehenem Einsatz können Zusatzfunktionen von Interesse sein, die viele NAS- Systeme anbieten: Verschlüsselung Backupfunktion	
Energieverbrauch	Üblich sind bis zu 20 W im Betrieb (mit 2 Festplatten) und bis zu 5W im Standby (HDD-Ruhezustand). Bei einigen NAS-Systemen lässt sich ein Sleep-Modus einstellen (max 1 W). Wenn das NAS im Sleep Modus ist, dauert der erste Zugriff länger (Starten des Systems, Hochfahren der Festplatten).	max. 20 W (Betrieb) max. 5 W (Standby) max. 1 W (Sleep-Modus)
Geräuschentwicklung	Falls das NAS in einem Raum steht, in dem sich gelegentlich Personen aufhalten, ist auf geräuscharme Systeme zu achten (Netzteil, Lüfter). Leistungsstarke NAS-Systeme sind üblicherweise	max. 19 dB (im Betriebsmodus, bei laufenden Festplatten)
Garantie	Gesetzlich garantiert sind 12 Monate. Optional kann zur Sicherstellung der für den Nutzer erforderlichen Wiederherstellungszeiten ein separater EVB-IT Vertrag abgeschlossen werden (innerhalb der gesetzlichen Garantiezeit und auch darüber hinaus).	Laufzeit EVB-IT Vertrag 1-5 Jahre Empfehlung: 3 Jahre

g) Beamer

Für die Lichterzeugung von Beamern gibt es unterschiedliche Technologien: Metalldampflampen sind derzeit die am häufigsten verwendeten Leuchtmittel bei Beamern. Sie enthalten jedoch Quecksilber. Die Lebensdauer von Metalldampflampen liegt typischerweise bei ca. 4000 Stunden, so dass ein gelegentlicher Lampenwechsel am Beamer erforderlich sein kann. Metalldampflampen benötigen eine Aufwärmphase und erreichen die volle Helligkeit erst nach ca. 1 Minute. LED-Beamer, Laser-Beamer oder kombinierte LED-/Laser-Beamer verwenden LED- bzw. Laserlichtquellen. Diese Leuchtmittel sind quecksilberfrei und haben eine Lebensdauer von typischerweise bis zu 20.000 Stunden. Die volle Helligkeit erreichen diese Beamer bereits nach wenigen Sekunden. Auch bezüglich des häufigen Ein-/Ausschaltens sind diese Beamer unempfindlich.

Datenblatt Beamer

Mindestkriterien: Werte für Lichtstärke, Auflösung, Schnittstellen

Aktuelle Beamer bieten verschiedene Helligkeitsstufen an (z. B. Normal-Modus und Eco-Modus). Bei der angegebenen Lichtstärke, bei der Lampenlebensdauer und beim Betriebsgeräusch muss die jeweilige Helligkeitsstufe betrachtet werden. Häufig wird in Datenblättern nur der jeweils günstigste Wert genannt.

Merkmal	Erläuterung / Hinweise	Werte
Lichtstärke	Auch für wechselnde Lichtverhält- nisse und nicht optimal geeignete Präsentati- onsflächen sollte der Beamer über eine ausreichende Helligkeit verfügen.	ab 3400 ANSI-Lumen (im Normal-Modus)
Auflösung	Idealerweise sollte die native Auflösung des Beamers der des Monitors entspre- chen. Für LED- Beamer, Laser-Beamer bzw. LED/Laser-Beamer und auch für Ultrakurzdistanz-Beamer sind derzeit aus Preisgründen bei der Auflösung noch Ab- striche zu machen.	Standard-Beamer ab 1920 x 1080 Pixel bzw. ab 1920 x 1200 Pixel LED- / Laser-Beamer ab 1280 x 720 Pixel bzw. ab 1280 x 800 Pixel Ultrakurzdistanz-Beamer ab 1280 x 720 Pixel bzw. ab 1280 x 800 Pixel
Lampenlebensdauer	Metalldampflampe: LED / Laser-Lichtquelle: LED / Laser-Lichtquellen können nicht gewechselt werden.	4000 Std. (Normal-Modus) 20.000 Std.
Schnittstellen	Aktueller Standard sind zwei HDMI- und ein VGA-Eingang.	2 digitale Schnittstellen (HDMI oder DisplayPort)
optionale Schnittstellen	Soll ein Adapter für die kabellose Bild- und Tonübertragung verwendet werden, wird dafür ein HDMI-Anschluss benötigt. Die Stromversorgung dieser Geräte kann über HDMI/MHL oder über USB erfolgen. In diesem Fall wird am USB-Port eine ausreichende Stromstärke (mind. 1,5 A) benötigt. Ein Netzwerkanschluss (LAN/WLAN) kann zur Steuerung des Beamers oder zur direkten Präsentation sinnvoll sein.	USB VGA, LAN, WLAN

Betriebsgeräusch	Die in den Datenblättern angegebenen Betriebsgeräusche sind nicht bei allen Anbietern exakt vergleichbar.	28 dB (Eco-Modus) 37 dB (Normal-Modus)
Garantie	Gesetzlich garantiert sind 12 Monate. Optional kann zur Sicherstellung der für den Nutzer erforderlichen Wiederherstellungszeiten ein separater EVB-IT Vertrag abgeschlossen werden (innerhalb der gesetzlichen Garantiezeit und auch darüber hinaus).	Laufzeit EVB-IT Vertrag 1-5 Jahre Empfehlung: 3 Jahre

Großbildmonitore

Neben speziellen Großbildmonitoren, die für den Dauerbetrieb ausgelegt sind, sind auch Consumer-Geräte (Fernseher) erhältlich, die jedoch hinsichtlich Helligkeit und Kontrast unter den hier angegebenen Werten liegen.

Datenblatt Großbildmonitor		
Mindestkriterien: Werte für Oberfläche und Helligkeit, Auflösung, Garantie		
Merkmal	Erläuterung / Hinweise	Werte
Oberfläche und Helligkeit	Für wechselnde Lichtverhältnisse sollte die Präsentationsfläche möglichst wenig spiegeln. Die Oberfläche sollte möglichst kratzunempfindlich sein (z. B. Mohs-Härtegrad 7). Es sollte darauf geachtet werden, dass ein Sicherheitsglas verwendet wird.	ab 350 cd/m² mattes Display gehärtetes Glas
Auflösung	Das Seitenverhältnis ist standardmäßig 16:9.	ab 3840 x 2160 Pixel
Lautsprecher	integrierte Lautsprecher	ab 2 x 10 W
Reaktionszeiten (Pixel)	Eine niedrige Reaktionszeit des Panels ist für die flüssige Darstellung von bewegten Inhalten notwendig.	maximal 8 ms

Schnittstellen	Um bei Bewegtbildern (> 30 Bilder/s) die volle Auflösung nutzen zu können sind HDMI 2.0-An-schlüsse erforderlich. Ansonsten genügen HDMI 1.4-Anschlüsse. 4K-Inhalte sind oft HDCP-2.2- geschützt. Für die Zuspielung durch externe Geräte, z. B. mit BluRay-Playern, muss der HDMI-Anschluss HDCP-2.2-fähig sein. Gegebenenfalls sind weitere Schnittstellen sinnvoll: • VGA (für ältere Notebooks) • Audio-Eingang • Audio-Ausgang • USB • Netzwerk	1 HDMI-2.0-Anschluss 1 weitere digitale Schnittstelle (HDMI oder DisplayPort)
Energieverbrauch	Der Energieverbrauch von Großbildmonitoren kann je nach Modell erheblich variieren.	
Drahtlosverbindung	Manche Monitore verfügen bereits über integrierte Möglichkeiten zur drahtlosen Bild- und Tonübertragung von mobilen Endgeräten aus.	
Garantie	Gesetzlich garantiert sind 12 Monate. Optional kann zur Sicherstellung der für den Nutzer erforderlichen Wiederherstellungszeiten ein separater EVB-IT Vertrag abgeschlossen werden (innerhalb der gesetzlichen Garantiezeit und auch darüber hinaus).	Laufzeit EVB-IT Vertrag 1-5 Jahre Empfehlung: 3 Jahre

Interaktive Großbildmonitore (Touchscreens)

Interaktive Großbildmonitore sollten von der Schule zusammen mit der voraussichtlich zum Einsatz kommenden Tafelsoftware getestet werden. Neben dem Handling der Stifte und dem subjektiven Schreibgefühl sollte vor allem auf die Verzögerung beim Schreiben und auf die Parallaxe beim Aufsetzen des Stifts geachtet werden.

Datenblatt Interaktiver Großbildmonitor (Touchscreen)		
Mindestkriterien: Werte wie bei Großbildmonitor		
Um einen PC an einen interaktiven Großbildmonitor anzuschließen, ist die Übertragung von Bild, Ton und Mausfunktionalität erforderlich. Dies kann auf folgende Arten erfolgen: - HDMI (Bild und Ton), USB (Mausfunktion), - OPS (Open Pluggable Specification, Bild-, Ton-, Mausfunktion) - VGA (Bild, eingeschränkte Auflösung), Klinke (Ton), USB (Mausfunktion) Der Anschluss mobiler Geräte (Tablets, Smartphones) erfolgt über integrierte Displayadapter (Bild- und Tonübertragung).		
Merkmal	Erläuterung / Hinweise	Werte
siehe Großbildmonitor	Alle Merkmale/Werte für nicht interaktive Großbildmonitore gelten auch für interaktive Großbildmonitore.	
Touchpunkte	Für Gestensteuerungen und gleichzeitiges Arbeiten muss das Display über Multitouch verfügen.	Display erfasst mindestens 8 gleichzeitige Berührungspunkte
Integrierter PC	Der Betrieb des interaktiven Großbildmonitors sollte über eine OPS-Schnittstelle (Open Pluggable Specification) erfolgen	
Onboard-Funktionen	Auch ohne angeschlossenen PC sollte der Großbildmonitor nutzbar sein.	Schreibfunktion (Tafel) Internet-Browser Mediaplayer
Energieverbrauch	Displays mit Infrarot-Technologie haben typischerweise einen höheren Energieverbrauch als kapazitive / induktive Technologien.	Infrarot-Technologie: typisch bis 500 W kapazitiv/induktiv: typisch bis 200 W

Dokumentenkameras

Dokumentenkameras (Visualizer) ermöglichen die Darstellung von Objekten über eine Großbilddarstellung. Sie ersetzen damit Tageslichtprojektoren und bieten darüber hinaus weitere Funktionen wie die Darstellung von Printmedien oder räumlicher Gegenstände.
Dokumentenkameras werden über einen Display-Anschluss (VGA oder HDMI) direkt mit dem Beamer verbunden und können auch ohne Computer betrieben werden.
Eine Möglichkeit zum Speichern von Arbeitsergebnissen (z. B. auf USB-Stick, Speicherkarte oder über den angeschlossenen PC) sollte vorgesehen sein. Moderne Dokumentenkamera lassen sich über WLAN in das Schulnetzwerk einbinden.

Datenblatt Dokumentenkamera		
Mindestkriterien: Werte für Auflösung, Bildfrequenz, Zoom, Schnittstellen		
Merkmal	Erläuterung / Hinweise	Werte
Auflösung	Die Ausgangsauflösung der Kamera sollte mindestens Full HD (1920 x 1080 Pixel) betragen. Dies entspricht ca. 2 Megapixel.	Ausgangsauflösung mind. 1920 x 1080 Pixel
Bildfrequenz	Für die Darstellung von Bewegtbildern sind mind. 30 Bilder/s nötig.	mind. 30 Bilder/s
Zoom	Digitalkameras bieten üblicherweise einen optischen und zusätzlich eine digitalen Zoom.	mind. 6-fach optischer Zoom
Schnittstellen	HDMI-Eingang zum Anschluss eines PC HDMI-Ausgang zum Beamer	HDMI-Eingang HDMI-Ausgang
optionale Anschlüsse		VGA, USB Cardreader
Lichtquelle		LED-Licht, abschaltbar
WLAN		802.11ac
Funktionen	Umschalter zwischen Dokumentenkamera, HDMI-Eingang bzw. VGA- Eingang (zur Darstellung eines angeschlossenen PC am Beamer, ggf. auch, wenn die Dokumentenkamera ausgeschaltet ist) Erstellen und Speichern von Bildern und Videos auf USB-Stick, Speicherkarte oder direkt auf den PC	

Drucker

Im Bereich der Schulverwaltung oder als zentraler Drucker für Lehrkräfte bietet es sich an, zum Drucken, Kopieren und Scannen zentrale Großgeräte (z. B. als Leasinggeräte) einzusetzen.
Als dezentraler Drucker mit geringem Druckvolumen ist ein netzwerkfähiger Monochrom- oder Farb-Seitendrucker empfehlenswert. Bei der Beschaffung sind die Verbrauchskosten (Gesamtkosten pro Seite bzw. monatliche Gesamtkosten) zu beachten.
Falls mobile Geräte (Tablets, Smartphones) einen Druckerzugriff haben sollen, sollte darauf geachtet werden, dass der Drucker auch die herstellerspezifischen Protokolle unterstützt (z.B. Apple AirPrint) bzw. cloudfähig ist (z. B. für Google Cloud-Print). Cloudbasierte Produkte sind datenschutzrechtlich anspruchsvoll (siehe 6.2).[71]

Datenblatt Drucker (dezentraler Drucker mit geringem Druckvolumen)		
Mindestkriterien: Werte für Auflösung, Schnittstellen		
Merkmal	Erläuterung / Hinweise	Werte
Typ, Format	Laser-/Tintenstrahldrucker, SW/Farbe, DIN A4 oder DIN A3	
Auflösung		ab 1200 x 1200 dpi
Geschwindigkeit		Zeit bis zur ersten Seite max. 30s mind. 30 Seiten/min nach ISO/IEC 24734:2014
Papierzufuhr	Für Einzelblätter (z. B. Briefumschläge, Folien) ist eine eigene Mehrzweckzufuhr sinnvoll.	Papierkassette 250 Blatt, Mehrzweckzufuhr
Duplex		Duplexdruck 10 Seiten/min
Schnittstellen	LAN-Anschluss, ggf. zusätzlich ein Wireless-LAN-Anschluss	RJ45 Ethernet (1 GBit/s)
Cloudbasierte Druckdienste	Cloudbasierte Druckdienste ermöglichen das Ausdrucken von mobilen Geräten aus, auch über das Internet, alternativ können die Dienste auch über einen PC freigegeben werden. Apple AirPrint, Google Cloud Print, herstellereigene Lösungen	
Zubehör	zweites bzw. größeres Papierfach	

[71] Siehe auch www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Publikationen/flyer-schulischer-datenschutz.pdf, Abrufdatum: 17.08.2019.

Ergonomie, Zertifizierung	„Energy Star“ beschreibt Mindestanforderungen für die Energieeffizienz. „Blauer Engel“ ist ein Umweltprüfzeichen mit Kriterien zu Energieverbrauch, Materialanforderungen, Recyclingfähigkeit und Geräuschemission.	Energy Star Blauer Engel (RAL-UZ 205 für Drucker)
Druckkosten	Druckkosten können bei den einzelnen Geräten stark schwanken.	s/w-Seite: < 2 Cent Farbseite: < 10 Cent

3D-Drucker

3D-Drucker eignen sich in der Schule zur Veranschaulichung räumlicher Strukturen (z. B. Prototypen bei CAD, räumliche Modelle in der Mathematik oder in den Naturwissenschaften, Gebäude- und Architekturmodelle in der Kunsterziehung).
Beim 3D-Druck wird das zu druckende Objekt Schicht für Schicht computergesteuert aufgebaut, um so dreidimensionale Werkstücke zu erzeugen. Die hierfür üblicherweise verwendeten Werkstoffe sind Kunststoffe, die geschmolzen und durch eine Düse gepresst werden.
Manche Materialien reagieren auf Temperaturschwankungen sehr empfindlich. Ein geschlossenes Druckersystem sorgt für weitgehend gleichbleibende Temperaturen während des Druckvorgangs und damit für präzisere Drucke. Zudem besteht die Möglichkeit, die beim Schmelzvorgang je nach verwendetem Material entstehenden Dämpfe gefiltert abzusaugen.
Für die Steuerung des Druckers wird eine entsprechende Software (Slicer) benötigt, welche meist mit dem Drucker mitgeliefert wird. Diese Software erstellt aus 3D-Körpern den entsprechenden Code mit Steuerbefehlen für den 3D-Drucker (z. B. g-code). Viele dieser Softwarepakete sind Open-Source und für verschiedene Drucker geeignet. Die Übermittlung der Daten erfolgt über einen USB-Anschluss oder durch Kopieren auf eine SD-Karte. Ebenso existieren Apps, die den Drucker per LAN oder WLAN steuern können.
Der 3D-Druck großer Werkstücke kann mitunter viele Stunden dauern. Eine Abschätzung der zu erwartenden Druckdauer liefert üblicherweise die Druckersoftware.
Für 3D-Drucker existieren auch viele Bausätze. Diese eigenen sich gut, um die Funktionsweise solcher Geräte kennen zu lernen. Für den produktiven Betrieb sind sie häufig nicht geeignet, da es ihnen oft an der nötigen Betriebssicherheit (u. a. CE) fehlt.
Für einen günstigen 3D-Druck kommt üblicherweise das Schmelzschichtverfahren (FDM: Fused Deposition Modelling, FLM: Fused Layer Modelling, FFF: Fused Filament Fabrication) zum Einsatz. Hier wird ein Werkstück aus geschmolzenem Kunststoff (Filament, z. B. PLA, ABS, PETG, Nylon, HIPS) bei Temperaturen von 150°C - 260°C schichtweise aufgetragen. Bei größeren Überhängen in dem zu druckenden Objekt sind Stützstrukturen notwendig, die anschließend entfernt werden müssen. Verfügt der Drucker über einen zweiten Druckkopf (Extruder), kann man diese Stützstrukturen aus einen wasserlöslichen Material (PVA) drucken, welches dann leicht und rückstandsfrei aufgelöst werden kann.
Bei zwei Extrudern ist es auch möglich, zweifarbig zu drucken. Mehrfarbige Drucke sind durch anschließendes Bedrucken des Werkstücks mit dem 3D-Tintenstrahl- verfahren möglich.
Damit sich das Werkstück während des Druckvorgangs nicht von der Druckplatte löst, gibt es verschiedene Möglichkeiten, die auch vom Druckmaterial abhängen. z. B. Glasplatte mit Haarspray, Pertinaxplatte, Blue Tape. Während man bei PLA auch bei unbeheizten Druckplatten gute Ergebnisse erzielen kann, ist bei anderen Werkstoffen wie ABS eine beheizbare Druckplatte erforderlich. Bei jedem Filament müssen die Temperatureinstellungen für Extruder und Druckplatte passend eingestellt werden.

Datenblatt 3D-Drucker		
Mindestkriterien: Werte für Schichtdicke, Druckplatte		
Merkmal	Erläuterung / Hinweise	Werte
Technologie	Schmelzschichtungs-Verfahren (FDM)	
Druckmaterial	Filament, Ø 1,75 mm oder Ø 2,85 mm, je nach Drucker. Die höhere Verbreitung hat Ø 1,75 mm. Kunststoffe: PLA, ABS, HIPS, PETG, Nylon, Tough PLA, Flex PLA, CPE, PVA u.a.	PLA oder ABS
Extruder	1-2 Extruder, wählbare Temperatur bis zu 260 °C Düsendurchmesser; 0,25 / 0,40 / 0,60 / 0,80 mm	Düsendurchmesser: 0,4 mm
Schichtdicke	ab 0,02 mm, u.a. abhängig von der gewählten Düse	bis 0,1 mm
Druckplatte	Auf der Druckplatte entsteht das Objekt. Für viele Kunststoffe ist eine beheizbare Druckplatte notwendig.	beheizbar
Objektgröße	abhängig von der Größe des Druckers und der Druckplatte Von 100 mm x 100 mm x 100 mm bis 500 mm x 500 mm x 500 mm und darüber hinaus möglich.	ca. 200 mm x 200 mm x 200 mm ist eine gängige Größe
Bauform	offen/geschlossen	geschlossen

Strukturierte Gebäudeverkabelung

Die nachfolgenden Empfehlungen für aktive Netzwerkkomponenten gehen von einer aktuellen Netzwerk-Infrastruktur aus, der eine strukturierte Gebäudeverkabelung zugrunde liegt (siehe auch Kapitel 6 Vernetzung der Rechner, Schulhausvernetzung). Insbesondere sind dies:

- Zentraler Serverraum im Schulgebäude (Gebäudehauptverteiler) mit breitbandiger Internetanbindung
- Mehrere Bereichsverteiler innerhalb der Schule
- Backbone-Verkabelung (zwischen Gebäudehauptverteiler und Bereichsverteiler) mit 10 GBit/s Glasfaser
- Verbindung zwischen Bereichsverteiler und Anschlussdosen am Arbeitsplatz mit 1 GBit/s Kupfer

Access-Points

Ein Access-Point ermöglicht den Zugriff auf das Schulnetz über WLAN. Bei mehreren Access-Points erleichtert ein Controller die Administration des Netzes. Zu unter- scheiden sind Standard-Access-Points (Fat-APs), die mit oder ohne Controller betrieben werden können und Access-Points, die ausschließlich im Zusammenspiel mit einem Controller betrieben werden können (Thin-APs). Bei Thin-APs läuft üblicherweise die gesamte WLAN-Kommunikation über den Controller (WLAN-Switch). Deshalb muss bei dieser Betriebsart auch das Netzwerk auf die zusätzliche Belastung ausgelegt sein.
Bei der Beschaffung sollte bereits auf die Möglichkeit der Erweiterung des Netzes geachtet werden (Skalierbarkeit). Der Einsatz professioneller Geräte ermöglicht den stabilen Betrieb auch bei vielen gleichzeitigen Zugriffen.

Datenblatt Access-Point		
Werte für WLAN-Standard, Übertragungsraten, Konfiguration, Authentifizierung, Multi-SSID, LAN-Schnittstelle, Strom- versorgung, Client-Isolation		
Merkmal	Erläuterung / Hinweise	Werte
WLAN-Standard	Aktueller Standard: 802.11ac (Wave 2) In der Regel bedienen diese Geräte neben 11ac-fähgen Geräten im 5 GHz-Band auch 11n-Clients im 2,4 GHz-Frequenzband.	IEEE 802.11ac 2,4 GHz und 5 GHz

Übertragungsraten	Übertragungsraten (802.11n- Standard im 2,4 GHz-Bereich): bis 150 MBit/s (Mimo 1x1) bis 300 MBit/s (Mimo 2x2) bis 450 MBit/s (Mimo 3x3) Übertragungsraten (802.11ac- Standard im 5 GHz-Bereich): bis 433 MBit/s (Mimo 1x1) bis 867 MBit/s (Mimo 2x2) bis 1300 MBit/s (Mimo 3x3)	2,4 GHz: ab 300 MBit/s 5 GHz: ab 867 MBit/s
Konfiguration	Gegebenenfalls sollte zusätzlich die Konfiguration über ein Webinterface möglich sein.	zentrales Management über einen WLAN- Controller möglich
Sendeleistung	Wenn externe Antennen angebracht werden, muss die Sendeleistung um den Antennengewinn reduziert werden. Um die Reichweite zu beschränken oder um Störungen zu benachbarten Access-Points zu vermeiden, kann es ebenfalls sinnvoll sein, die Sendeleistung zu reduzieren.	Die maximale Sendeleistung sollte reduzierbar sein.
Authentifizierung	Üblich sind heute WPA2-PSK (Preshared Key) und WPA2-Enterprise (802.1x in Verbindung mit einem Radius-Server).	WPA2-PSK und WPA2-Enterprise (802.1x)
Multi-SSID	Multi-SSID ermöglicht die Bereitstellung mehrerer Funkzellen (SSIDs) in unterschiedlichen Teilnetzen (VLANs) für unterschiedliche Benutzergruppen (z. B. Lehrer, Schüler, etc.)	Multi-SSID VLAN-Unterstützung nach 802.1q
LAN-Schnittstelle	Ggf. können auch 2 LAN- Schnittstellen sinnvoll sein (z.B. separate Konfigurationsschnittstelle).	1 GBit/s-Ethernet
Stromversorgung	PoE (Power-over-Ethernet) ist Standard. Gegebenenfalls zusätzlich externes Netzteil	PoE 802.3af oder 802.3at
Antennen	Externe Antennen können durch spezielle Richtcharakteristiken das Sende- und Empfangsverhalten positiv beeinflussen; im Klassenzimmer reichen meist die eingebauten Standardantennen (Rundstrahler).	
Client-Isolation	Beim Betrieb des Access-Points als Hotspot ist es sinnvoll, die Kommunikation der WLAN-Clients untereinander zu unterbinden. Oft führt dies jedoch zu Schwierigkeiten bei der drahtlosen Bildschirmübertragung oder beim drahtlosen Drucken.	Client-Isolation einstellbar

Ergonomie / EMV	Durch die EMV-Zertifizierung (Elektromagnetische Verträglichkeit) nach EN 60601-1-2 ist ein Access-Point auch für den Einsatz in medizinischen Umgebungen zugelassen.	EMV-Zertifizierung nach EN 60601-1-2
Garantie	Gesetzlich garantiert sind 12 Monate. Optional kann zur Sicherstellung der für den Nutzer erforderlichen Wiederherstellungszeiten ein separater EVB-IT Vertrag abgeschlossen werden (innerhalb der gesetzlichen Garantiezeit und auch darüber hinaus).	Laufzeit EVB-IT Vertrag 1-5 Jahre Empfehlung: 3 Jahre
Service	Der Hersteller sollte über eine gut gepflegte (eventuell deutschsprachige) Internetpräsenz verfügen und darüber kostenlos Firmware-Updates, Datenblätter und Zusatzinfos (z.B. Konfigurationsbeispiele) anbieten.	Kostenfreie Versorgung mit Firmware-Updates

WLAN-Controller

Ein WLAN-Controller ermöglicht die zentrale Konfiguration, das zentrale Management und ein übersichtliches Monitoring der WLAN-Access-Points in einem Netz. Die Funktionsweise des WLAN-Controllers ist herstellerabhängig. Auch arbeiten WLAN- Controller üblicherweise nur mit Access-Points des gleichen Herstellers zusammen. Service und Support sollten langfristig sichergestellt sein.

Übersicht zu WLAN-Controllern	
Funktionsweise eines WLAN-Controllers	
Management eigenständiger Access-Points (Fat-APs)	Der Controller dient nur zur Konfiguration und zur Überwachung der Access-Points. Ansonsten sind die Access-Points eigenständig und funktionieren auch ohne Controller. Die WLAN-Nutzdaten laufen nicht über den Controller.
Zentrale Komponente für den Betrieb von Thin-APs	Die Access-Points können nicht eigenständig betrieben werden. Alle WLAN-Nutzdaten laufen über den Controller bzw. einen eigenen WLAN-Switch.
Implementierung von WLAN-Controllern	
eigenständiger Hardware- Controller (Appliance)	Der Controller ist ein eigenes Gerät. Dies ist üblich, wenn alle WLAN-Nutzdaten über den Controller laufen.
Zusatzfunktion auf einem Router oder Access-Point	Der Controller ist ein Zusatzdienst auf einem Access- Point oder Router. Gegebenenfalls muss dieser Dienst eigens lizenziert werden.
Serverdienst	Der Controller wird als Software auf einem Windows- oder Linux-Server installiert.
Cloud-Service	Der Controller wird teilweise als Cloud-Service angeboten. Diese Variante ist gegebenenfalls auch mandantenfähig und ermöglicht das zentrale Management mehrerer Standorte bzw. Schulen. Zur Konfiguration benötigen die Access-Points eine Internetverbindung. Üblicherweise entstehen hier auch Kosten für den Betrieb des Cloud-Service. Externe Clouddienste bedürfen einer Risikoanalyse bezüglich Sicherheit und Datenschutz.[72]

[72] Siehe dazu www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Publikationen/flyer-schulischer-datenschutz.pdf, Abrufdatum: 18.08.2019.

Funktionen eines WLAN-Controllers	
übliche Funktionen	□ automatische Erkennung neuer Access-Points □ zentrale Konfiguration aller Access-Points □ zentrales Monitoring aller Access-Points automatisches Firmware-Rollout für alle Access- Points
optionale Funktionen	□ Betrieb einer Captive-Portal-Lösung Benachrichtigung per E-Mail, wenn Fehler auftreten

Ethernet-Switche

Eine Netzwerk-Infrastruktur wird mit managebaren VLAN-fähigen Layer-2-Switchen und gegebenenfalls mit einem zentralen Layer-3-Switch (mit Routing- und Firewall- funktionen) aufgebaut. Nicht managebare Switche können in kleineren Umgebungen oder zur Versorgung von POE-fähigen Geräten zum Einsatz kommen.

Datenblatt Ethernet-Switch (managebarer VLAN-fähiger Layer-2-Switch zum Einsatz in einem Bereichsverteiler)		
Mindestkriterien: Werte für Anschlüsse, VLANs, Leistung, Garantie		
Merkmal	Erläuterung / Hinweise	Werte
Konfiguration	Die übliche Konfiguration erfolgt über ein Webinterface des Routers. Ein Konsolenanschluss ermöglicht einen Zugang unabhängig von der IP-Konfiguration. Neue Technologien setzen auf die Möglichkeit einer cloudbasierten Konfiguration der Geräte (siehe dazu 6.2).	Konfiguration über ein Webinterface
Anschlüsse	Üblich sind 24 oder 48 Ethernet- Ports (RJ45) mit 10/100/1000 MBit/s (Autosensing) und zusätzlich 2-4 Uplink-Ports mit 1 GBit/s SFP oder 10 GBit/s SFP+.	ab 24 Ethernet-Ports mit 10/100/1000 MBit/s ab 2 SFP+ Ports mit 10 GBit/s
PoE	Zur Stromversorgung angeschlossener Netzwerkgeräte (z. B. WLAN- Access-Points, IP-Telefone, Web- Kameras) ist PoE (Power over Ethernet) Standard. PoE nach IEEE 802.3af: (max. Leistung pro Port: 15,4 W) PoE+ nach IEEE 802.3at (max. Leistung pro Port: 30 W) Die PoE-Gesamtleistung sollte über der benötigten Leistung liegen.	PoE+ nach IEEE 802.3at PoE+-Gesamtleistung: mind. 300W
VLANs		VLAN-Unterstützung nach 802.1Q

zusätzliche Funktionen	Rapid Spanning-Tree (Loop- Protection) ggf. QoS (Quality of Service) bei VoIP ggf. Port-Mirroring und Protokollierung fehlerhafter Datenframes (Fehlersuche) ggf. Link Aggregation (Bündeln von Uplink-Ports für höhere Bandbreiten)	
Status-Anzeigen		Verschiedenfarbige LED- Leuchten für Status-, Aktivitäts- und Geschwindigkeitsanzeige des jeweiligen Ethernet-Ports
Montage	Montage im Rack	19 Zoll-Gerät
Leistung	Die interne Switching-Kapazität (Bandbreite der Backplane) sollte der (doppelten) Gesamtkapazität aller Ports entsprechen. Der Datendurchsatz in Mpps (Million Packets per Second) gibt an, wie viele Pakete der Switch verarbeiten kann (üblicherweise mit 64 Byte-Paketen gemessen). Eine sinnvolle Größenordnung für den erforderlichen Datendurchsatz kann man aus der Switching-Kapazität ermitteln, wenn man mit einer durchschnittlichen Paketgröße von 2000 Bit kalkuliert. Weitere Leistungsparameter können sein: Latenzzeit, Paketpuffergröße Nicht alle Anbieter geben vergleichbare Werte für die Leistungsfähigkeit an.	Switch mit 24 Ethernet- und 2 SFP+-Ports: Switching-Kapazität: 88 GBit/s Datendurchsatz: mind. 44 Mpps Switch mit 48 Ethernet- und 4 SFP+-Ports: Switching-Kapazität: 176 GBit/s Datendurchsatz: mind. 88 Mpps
Garantie	Gesetzlich garantiert sind 12 Monate. Optional kann zur Sicherstellung der für den Nutzer erforderlichen Wiederherstellungszeiten ein separater EVB-IT Vertrag abgeschlossen werden (innerhalb der gesetzlichen Garantiezeit und auch darüber hinaus).	Laufzeit EVB-IT Vertrag 1-5 Jahre Empfehlung: 3 Jahre
Service	kostenfreie Versorgung mit Firmware-Updates, Serviceadresse	

Layer-3-Switche

In großen schulischen Netzwerken (z. B. differenzierte Aufteilung des lokalen Netzes in Teilnetze mit Unterrichtsnetz, Lehrernetz, Verwaltungsnetz, WLAN-Netze, etc.) kann ein zentraler Layer-3-Switch, der das schulinterne Routing übernimmt, sinnvoll sein.
Bei einer weniger differenzierten Aufteilung des lokalen Netzes (z. B. Unterrichtsnetz, Lehrernetz) kann diese Aufgabe auch der Internetzugangsrouter mit übernehmen.

Datenblatt Layer-3-Switch		
Mindestkriterien: Werte wie beim Layer-2-Switch		
Merkmal	Erläuterung / Hinweise	Werte
Layer-2 Merkmale	Alle Merkmale für Layer-2-Switche gelten auch für Layer-3-Switche.	
Leistung	Layer-3-Switche unterscheiden beim Datendurchsatz nicht zwischen Routing und Switching. Die interne Switching-/Routing- Kapazität (Backplane) sollte der (doppelten) Gesamtkapazität aller Ports entsprechen.	
Routing		statisches Routing
Firewall		ACL-Filterung basierend auf Ziel/Quell-IP auf VLAN-Basis
mögliche zusätzliche Funktionen	DHCP-Server DHCP-Relay (Weiterleitung von DHCP-Anfragen) QoS (Quality of Service) bei VoIP Bandbreitenbeschränkung per Port	

Internetzugangsrouter

Ein Internetzugangsrouter (Access-Router) verbindet das Schulnetz mit dem Internet. Der Router bietet dazu Übergänge vom lokalen Netz (auf Ethernet-Basis) auf ein Weitverkehrsnetz (DSL, Kabelnetz). Dieser Übergang ist eine wichtige Schnittstelle und erfordert eine präzise Konfiguration und eine stabile Funktion.
Professionelle Router, wie sie überwiegend im kommerziellen Umfeld eingesetzt werden, bieten differenzierte Firewall-Funktionen. Speziell für Schulen werden auch vorkonfigurierte Kommunikationsserver angeboten (Computer auf Linux-Basis). Bei diesen ist zu prüfen, ob sie den Erfordernissen der Schule bzw. den nachfolgenden Empfehlungen im Datenblatt (z. B. Routing-Durchsatz) genügen.
Einfache DSL-Router, wie sie im privaten Bereich eingesetzt werden, sind für die meisten Schulen nicht geeignet, da diese nicht für den Internetanschluss von mehreren hundert Geräten ausgelegt sind, nur ein lokales Netz verwalten können und keine differenziert konfigurierbare Firewall besitzen.
Nachfolgend ist ein schulgeeigneter Hardware-Router beschrieben.

Datenblatt Internetzugangsrouter		
Mindestkriterien: Werte für LAN-Schnittstellen, WAN-Schnittstellen, Routing- Durchsatz		
Merkmal	Erläuterung / Hinweise	Werte
Konfiguration	Die übliche Konfiguration erfolgt über ein Webinterface des Routers. Ein Konsolenanschluss ermöglicht einen Zugang unabhängig von der IP- Konfiguration. Neue Technologien setzen auf die Möglichkeit einer cloud-basierten Konfiguration der Geräte (siehe dazu 6.2).	Konfiguration über ein Webinterface
LAN-Schnittstellen	4 x 1 Gigabit-Ethernet-Ports, die als Router-Ports in unterschiedliche Netze getrennt werden können (z. B. Unterrichtsnetz, Lehrernetz, Verwaltungsnetz). Einzelne LAN-Ports können in Verbindung mit einem externen Modem auch als zusätzliche WAN-Schnittstellen geschaltet werden (z. B. für load-balancing).	4 x 1 GBit/s-Ethernet-Ports, als Router-Ports konfigurierbar

WAN- Schnittstellen	Eine oder mehrere WAN Gigabit-Ethernet-Schnittstellen, konfigurierbar für externes Modem (z. B. PPPoE, je nach Provider) z. B. DSL-Schnittstelle mit integriertem Modem für ADSL/ADSL2+, VDSL, SDSL (Annex B/J), LWL	1 zur WAN-Technologie kompatible Schnittstelle (z.B. DSL, Kabel, Ethernet)
VLANs	Zusätzlich zu den physikalischen Schnittstellen lassen sich Subinterfaces bzw. VLANs konfigurieren, über die weitere Teilnetze angesprochen werden können.	Unterstützung von VLANs nach 802.1q, Routing zwischen VLANs
Firewall	Eine Stateful-Inspection-Firewall ermöglicht die richtungsabhängige Paketfilterung und Überwachung des Status der einzelnen Verbindung. Die Firewall muss konfigurierbar sein nach Quelle, Ziel und Dienst (IP- Adressen, Schnittstellen, Ports).	Stateful Inspection Firewall, konfigurierbar nach Quelle, Ziel, Dienst
Routing-Durchsatz	Wenn der Router auch zur Trennung verschiedener Netze (z. B. Unterrichts- netz, Lehrernetz, Verwaltungsnetz) eingesetzt werden soll, sollte der Durchsatz entsprechend höher sein.	Routing-Durchsatz mind. 800 MBit/s
VPN	VPN-Verbindungen (über IPSEC, SSL oder L2TP) ermöglichen einen sicheren Remote-Zugriff über das Internet (z. B. zur Fernwartung, Anschluss einer Zweigstelle, Remote-Zugriff einzelner Lehrkräfte). Gegebenenfalls ist eine eigene VPN-Client-Software erforderlich. Wenn viele gleichzeitige VPN-Verbindungen nötig sind, erfordert dies einen leistungsstärkeren (und teureren) Router.	Unterstützung von 5 gleichzeitigen VPN- Verbindungen über IPSEC
DNS, DHCP, etc.	Weitere Zusatzfunktionen (DNS Relay bzw. DNS Proxy, DHCP, Dynamisches DNS) sind üblicherweise an allen Routern integriert.	DHCP-Server für alle Teilnetze, DNS-Relay
Jugendschutzfilter	Viele Internetzugangsrouter bieten eine Unterstützung für die Nutzung eines Jugendschutzfilters (Webfilter auf DNS- Basis). Dieser muss üblicherweise eigens lizenziert werden.	
Hotspot-Gateway	Einige Router bieten ein Hotspot- Gateway an (z. B. für ein Schüler- oder Gäste-WLAN). Die Authentifizierung erfolgt über einen Radius-Server, der ggf. lizenziert werden muss.	

Montage	19"-Zoll-Gerät zum Einbau in einem Rack, bzw. Tischgerät	19"-Gerät bzw. 19"-Einbaurahmen
Garantie	Gesetzlich garantiert sind 12 Monate. Optional kann zur Sicherstellung der für den Nutzer erforderlichen Wiederherstellungszeiten ein separater EVB-IT Vertrag abgeschlossen werden (innerhalb der gesetzlichen Garantiezeit und auch darüber hinaus).	Laufzeit EVB-IT Vertrag 1-5 Jahre Empfehlung: 3 Jahre
Service	Der Hersteller sollte über eine gut gepflegte (eventuell deutschsprachige) Internetpräsenz verfügen und darüber kostenlos Firmware-Updates, Datenblätter und Zusatzinfos (z. B. Konfigurationsbeispiele) anbieten.	Kostenfreie Versorgung mit Firmware-Updates

Glossar

Access Point

Access Point bieten ein WLAN an und fungieren damit als Basiseinheit für damit verbundene mobile Endgeräte. Im Regelfall werden Access Points über ein LAN mit dem lokalen Netz und dem Internet verbunden. Professionelle AP's werden zentral verwaltet und bieten auch die Möglichkeit, über verschiedene SSID's mehrere getrennte Netze (VLAN's) anzubieten.

AirPlay

AirPlay ist eine proprietäre Schnittstelle zur kabellosen Übertragung von Inhalten von iOS- und OS X-Geräten über die Software iTunes auf AirPlay-fähige Empfängergeräte wie Lautsprecher, AV-Empfänger, Stereosysteme und Fernseher.

Authentifizierung

Authentifizierung ist der Nachweis (Verifizierung) einer behaupteten Eigenschaft einer Entität, die beispielsweise ein Mensch, ein Gerät, ein Dokument oder eine Information sein kann, und die dabei durch ihren Beitrag ihre Authentisierung durchführt.

Backbone

Das Backbone-Netz ist ein Hochleistungsnetz magistralen Charakters (Hauptnetz), das den Anschluss einer Vielzahl von territorial verteilten Endgeräten, Endgeräte-Clustern oder lokalen Subnetzen erlaubt wie Lokale Netze (LAN), Nebenstellenanlagen und Terminalnetze, und diese Netze und Systeme untereinander verbindet.

Backup (Datensicherung)

Eine inkrementelle oder vollständige Sicherung von Dateien, Verzeichnissen oder ganzen Datenträgern hilft Datenverlusten vorzubeugen.

Breitband

Unter Breitband versteht man ein Internetzugang mit einer hohen Datenübertragungsrate.

Captive Portal

Über ein Captive Portal besteht die Möglichkeit, den Zugriff auf ein Netzwerk, im Regelfall auf das Internet, zu steuern. Nach dem Verbinden mit einem LAN oder WLAN wird der Nutzer, die Nutzerin auf eine spezielle Website umgeleitet, welche die Eingabe von Benutzerdaten abfordert. Das Log-Out erfolgt zeitgesteuert oder über eine manuelle Abmeldung.

Cloud-Computing

Cloud Computing beschreibt einen internetzentrierten Entwicklungsansatz, bei dem ein Anbieter komplexe Leistungen aus Soft- und Hardware in Form eines abstrakten Dienstes bereitstellt. Speicher, Rechenzeit oder komplexere Dienste können über festgelegte Schnittstellen abgefordert werden, wobei es keine Rolle spielt, auf welcher Hardware diese letztendlich ausgeführt werden.

Fediverse

Fediverse ist ein Kofferwort aus „federation“ und „universe“ und bezeichnet ein Netzwerk föderierter, voneinander unabhängiger sozialer Netzwerke, Mikroblogging-Diensten und Webseiten für Online-Publikation oder Daten-Hosting

Gateway

Als Gateway bezeichnet man Geräte, die Netze mit unterschiedlicher Kommuni-kationsarchitektur (bzw. auf dem Niveau der niedrigsten Hierarchieschicht) verbinden.

Hot-Swap

Ein Qualitätsmerkmal eines RAID-Systems ist, dass die Festplatten im laufenden Betrieb ausgewechselt werden können und somit der Datenzugriff nicht unterbrochen werden muss.

Intrusion Prevention

DasIntrusion Prevention System (IPS) dient der Identifikation von Anwendungen und Protokollen unabhängig vom genutzten Port und der Berücksichtigung externer Datenquellen, wie zum Beispiel Verzeichnisdienste mit Benutzerdaten.

IP-Adresse

Die IP-Adresse ist eine netzweit eindeutige logische Adresse für das IP-Protokoll.

LAN (Lokales Netz, Local Area Network)

Das LAN ist ein Kommunikationssystem mit territorial beschränkter Ausdehnung (Etage, Gebäude, Campus) und einer Reihe kommunikationstechnischer Besonderheiten.

MAC-Adresse

Die MAC-Adresse ist eine individuelle Hardware-Adresse jedes einzelnen Netzwerkadapters (Netzwerkkarte) zur eindeutigen Identifikation des Gerätes im Netz. Bei Ethernet ist sie 48 bit lang. Anhand von MAC-Adressen können MAC-Frames ihr Ziel erreichen, wenn die Ziel-MAC-Adresse in einem Frame mit der MAC-Adresse eines Computers im LAN übereinstimmt. MAC-Adressen und MAC-Adressierung sind Bestandteil von OSI-Schicht 2.

MAC-Adressen-Filterung

Mithilfe der MAC-Adressen-Filterung werden nur Geräte mit bekannten MAC-Adressen in einem Netzwerk zugelassen. Sie stellt damit eine Sicherheitsstufe dar, mit der verhindert werden soll, dass sich unbefugte Computer in einem Netzwerk befinden. Da sich die MAC- Adresse jedoch ändern lässt, ist eine MAC-Adressen-Filterung als alleiniger Sicherheitsmechanismus nicht ausreichend.

MIMO

Als MIMO oder Multiple Input Multiple Output (engl. für mehrfache Eingabe/mehrfache Ausgabe) wird eine Funktechnologie bezeichnet, bei der mehrere Sende- und Empfangsantennen benutzt werden, um eine optimale Übertragungsleistung zu erzielen.

Miracast

Miracast ist ein Peer-to-Peer-Funk-Screencast-Standard, der von der Wi-Fi Alliance definiert wurde. Er wird als offener Standard gegenüber Apples AirPlay, Samsungs Screen Mirroring und Intels Wireless Display (WiDi) angesehen, obwohl die Spezifikationen des Standards Entwicklern nur nach der Bezahlung eines hohen Geldbetrages zur Verfügung gestellt werden. Der Standard ermöglicht zum Beispiel, den Bildschirminhalt eines Smartphones oder eines Rechners, etwa für Präsentationen, auf einen großen Monitor oder Videoprojektor zu übertragen.

Radius-Server

Ein Radius-Server stellt einen zentralen Authentifizierungsdienst zur Verfügung, bei dem sich der Nutzer, die Nutzerin z. B. in einem WLAN anmelden kann. Dieser kann auch an eine vorhandene Benutzerdatenbank bzw. an einen vorhandenen Verzeichnisdienst angebunden sein.

Secure Shell (SSH)

SSH ist ein Protokoll zur Anmeldung auf einem entfernten Rechner. Die Kommunikation erfolgt verschlüsselt und kann daher als sicher erachtet werden. SSH ist Telnet vorzuziehen.

Shared Service

Shared Service ist ein Organisationsmodell, mit dem Dienstleistungen (Services) der zentralen Verwaltung und deren Verwaltungsbereiche, Verwaltungseinheiten oder Abteilungen verknüpft und in einer spezifischen, kundenorientierten Organisationseinheit (Center) zusammengefasst werden. Auf diese Services können die einzelnen Verwaltungsbereiche, Verwaltungseinheiten oder Abteilungen dann nach Bedarf (shared) zugreifen.

Skalierbarkeit

Unter Skalierbarkeit versteht man im Bereich der IKT-Infrastruktur die Fähigkeit eines Systems aus Hard- und Software, die Leistung durch das Hinzufügen von Ressourcen in einem definierten Bereich proportional (bzw. linear) zu steigern.

Stateful Inspection

Stateful Inspection ist ein Firewall-Leistungsmerkmal. Dieses Verfahren entscheidet anhand mehrerer Kriterien, ob ein eingehendes Datenpaket weitergeleitet oder verworfen wird. Z. B. wird der Zielport als Kriterium verwendet. Ist in der Firewall für diesen Port kein Server angegeben, werden die Datenpakete für diesen Port verworfen. Zudem wird überprüft, ob eingehende Datenpakete zu zuvor gesendeten Datenpaketen in Beziehung stehen.

Telnet

TelNet ist das grundlegende Protokoll zur Anmeldung auf einem entfernten Rechner. Es bietet keinerlei Sicherheitsfunktionen, insbesondere werden Passwörter im Klartext übertragen. Daher ist SSH Telnet vorzuziehen.

Thin-Client

Ein Thin-Client enthält lediglich eine Benutzeroberfläche sowie Funktionen zur Kommunikation mit seinem Server.

Virtual Private Network (VPN)

VPN ist ein logisches privates Netzwerk auf einer öffentlich zugänglichen Infrastruktur. Nur die Kommunikationspartner, die zu diesem privaten Netzwerk gehören, können miteinander kommunizieren und Informationen und Daten austauschen.

Virtualisierung

Unter Virtualisierung versteht man Methoden zur Abstraktion, die es erlauben, dem Benutzer scheinbar vorhandene Ressourcen so verfügbar zu machen, als wären sie real vorhanden.

VLAN (Virtual LAN)

Das VLAN ist ein virtuelles lokales Netz mit gemeinsamem Adressraum, das durch Zusammenschalten von LAN-Komponenten aus verschiedenen LAN-Segmenten entsteht.

WAN (Wide Area Network, Weitverkehrsnetz)

Ein WAN ist ein Kommunikationsnetz für die Überbrückung größerer Entfernungen. z. B. Land, Kontinent, interkontinental.