Schleswig-Holstein
Ministerium für Bildung,
Wissenschaft und Kultur

Basis-Informationssicherheitskonzept

für die öffentlichen Schulen in Schleswig-Holstein

Version 1.1 vom 15.04.2020

April 2020

Schleswig-Holstein. Der echte Norden

Impressum

Basis-Informationssicherheitskonzept für die öffentlichen Schulen in Schleswig-Holstein

Herausgeber:

Ministerium für Bildung, Wissenschaft und Kultur

des Landes Schleswig-Holstein

Brunswiker Str. 16-22

24105 Kiel

Historie der Dokumentversionen

Version	Status	Datum	Autor	Änderungsgrund / Bemerkungen
0.1	Entwurf	18.02.2019	Manuel Carl	Erste Befüllung
0.2	Entwurf	21.02.2019	Manuel Carl	Einarbeitung Kommentare Martin Möller Kapitel 1
0.3	Entwurf	26.02.2019	Manuel Carl	Einarbeitung Kommentare Martin Möller Kapitel 2
0.4	Entwurf	08.03.2019	Manuel Carl	Einarbeitung Kommentare Martin Möller Kapitel 3
0.5	Entwurf	02.05.2019	Manuel Carl	Einarbeitung Kommentare Martin Möller Kapitel 4
0.6	Entwurf	06.06.2019	Manuel Carl	Einarbeitung Kommentare Jan Tröster
0.7	Entwurf	12.06.2019	Manuel Carl	Einarbeitung Kommentare Martin Möller Kapitel 5
0.8	Entwurf	13.06.2019	Manuel Carl	Einarbeitung Kapitel „Einführung“
0.9	Entwurf	14.06.2019	Manuel Carl	Review Prozess
1.0	Finale Version	28.06.2019	Manuel Carl	Übergabeversion
1.1	Veröffentlichungs-fassung	15.04.2020	III DSB/S	Layoutanpassungen, Schärfung von Formulierungen, Korrektur von Rechtsquellen

Inhaltsverzeichnis

Tabellenverzeichnis

Vorwort

Sehr geehrte Schulleiterinnen und Schulleiter,

Informationssicherheit und insbesondere die IT-Sicherheit sind in den letzten Jahren zu Schlagwörtern in den Medien geworden. Durch die zunehmende Digitalisierung von Verwaltungsabläufen sowie vermehrten und stetig komplizierteren Hacker-Angriffen wird der Schutz von Informationen immer wichtiger und macht vor den Schulen in Schleswig-Holstein keinen Halt. Aufgrund der komplexen Zusammenhänge in den Themenfeldern Informationssicherheit und dem Teilgebiet Datenschutz ist es jedoch schwierig den Überblick über die Schwerpunkte zu erhalten.

Allen voran steht in den Schulen der Umgang mit personenbezogenen Daten im Fokus der Lehrkräfte und Eltern, was mit dem Inkrafttreten der EU-DSGVO in besonderen Maßen an Bedeutung gewonnen hat. Dabei ist zu berücksichtigen, dass die Schulen naturgemäß überwiegend personenbezogene Daten von minderjährigen Schülerinnen und Schülern verarbeitet werden. Dabei handelt es sich auch um besondere Kategorien von Daten, wie etwa Angaben zu der religiösen Zugehörigkeit oder gesundheitlicher Besonderheiten. Diese sind gesetzlich verordnet im besonderen Maße zu schützen. Darüber hinaus sind die meisten Schulen in Schleswig-Holstein formal als Behörden anzusehen und unterliegen somit den gesetzlichen Vorgaben der Informationssicherheit für öffentliche Stellen.

Das Ministerium für Bildung, Wissenschaft und Kultur (MBWK) hat in der Zusammenarbeit mit dem Bereich Digitale Agenda und zentrales IT-Management der Landesregierung (ZIT SH) des Ministeriums für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung (MELUND) im Rahmen des Projektes DaSch Unterstützungsmaterialien für die Schulen in Schleswig-Holstein erarbeitet. Diese sollen Sie bei der Implementierung der verpflichtenden Datenschutzdokumentation unterstützen. Dazu zählt auch das vorliegende Basis-Informationssicherheitskonzept für die Schulen, für das insbesondere die Basis-Anforderungen des BSI-Grundschutz-Kompendiums sowie Vorgaben des IQSH, des MBWK und des ULD als Grundlage dienten.

Das Basis-Informationssicherheitskonzept dient zur Orientierung und bildet Eckpfeiler der Informationssicherheit ab, die für die Schulen in Schleswig-Holstein relevant sind. Es ist eine Basis für die Implementierung von Maßnahmen zum Schutz der personenbezogenen Daten in den Schulen und nimmt neben den technischen insbesondere die nichttechnischen Anforderungen der Informationssicherheit in den Fokus. Es hat das Ziel, den Schulen einen fachlichen Rahmen zu geben, um die Sicherheit der Informationen eigenständig organisieren und aufbauen zu können. Darüber hinaus kann das Basis-Informationssicherheitskonzept flexibel an die Rahmenbedingungen und Anforderungen der jeweiligen Schule angepasst werden.

Aufbau des Konzeptes

Das Konzept ist in insgesamt fünf Kapitel untergliedert, die in der nachfolgenden Tabelle kurz beschrieben werden.

Kapitel	Erläuterung
1	Das erste Kapitel umfasst Grundsätze und Ziele der Informationssicherheit und beschreibt die übergreifenden Verantwortlichkeiten in der jeweiligen Schule.
2	Das zweite Kapitel legt Informationsklassen anhand von Beispielen fest und stellt Anforderungen, wie mit den jeweiligen Klassen umzugehen ist. Weiterhin geht es auf personenbezogene Daten im Sinne der EU-DSGVO ein.
3	Das dritte Kapitel beschäftigt sich mit der allgemeinen Informationssicherheit. Dazu zählen Gebäude- und Raum-Zutritte, Tresore, der Umgang mit Ablagesystemen (Aktenaufbewahrung), der Umgang mit Sicherheitsvorfällen und ein Mindestmaß an Notfallvorsorge.
4	Das vierte Kapitel gibt Vorgaben für mitarbeiternahe Prozesse, wie der Sensibilisierung zum Thema Informationssicherheit, der Vergabe und Verwaltung von Berechtigungen, Einarbeitung sowie Austritten von Mitarbeitern.
5	Das fünfte Kapitel geht auf die IT-Sicherheit in den Schulen ein und gibt grundlegende Vorgaben zur Nutzung von Hardware-Komponenten, wie Rechnern, mobilen Endgeräten sowie mit Software-Produkten, wie der Schulverwaltungssoftware.

Tabelle 1: Kapitelübersicht

Umgang mit dem Konzept

Die Nutzung dieses Basis-Informationssicherheitskonzeptes durch die Schulen ist nicht verpflichtend. Gleichwohl stellt es eine Empfehlung und Unterstützung dar, die durch die Schule freiwillig in Anspruch genommen werden kann, um die Informationssicherheit zu strukturieren und zu verbessern. Ein Informationssicherheitskonzept ist allerdings im Rahmen der Dokumentationspflichten vorzuhalten. Bitte berücksichtigen Sie, dass die Implementierung der Informationssicherheit in eine Organisation nicht innerhalb weniger Tage getan und vollumfänglich abgeschlossen ist. Vielmehr handelt es sich um einen kontinuierlichen Verbesserungsprozess. Daher ist die Implementierung eine fortlaufende Aufgabe.

Der Grundgedanke des vorliegenden Konzeptes ist, dass die Schule das Dokument als ein für sie geltendes Konzept annimmt, an seine eigenen Bedürfnisse und Rahmenbedingungen anpasst und seine Umsetzung eigenverantwortlich durchführt.

Innerhalb der Kapitel 1 bis 5 werden dazu Anforderungen gestellt, die durch die Schule umgesetzt werden. An passenden Stellen des Dokumentes sind darüber hinaus Checklisten angeführt. Die Anforderungen in den Checklisten sind i.d.R. zunehmend anspruchsvoller. Die Schule kann dabei selbst entscheiden, welche der Anforderungen für sie relevant sind und kreuzt die entsprechenden Anforderungen in der jeweiligen Checkliste mit „Ja“ oder „Nein“ an. Anforderungen die mit „Ja“ angekreuzt werden, sind für die Schule relevant und wurden umgesetzt oder deren Umsetzung ist geplant. Anforderungen, die mit „Nein“ angekreuzt sind, werden zunächst nicht weiter betrachtet. Je geringer die Anzahl der mit „Nein“ angekreuzten Checklistenelemente, je höher ist der Reifegrad einer Schule in Bezug zur

Informationssicherheit anzusehen, soweit die mit „Ja“ angekreuzten Anforderungen umgesetzt wurden.

Im Laufe des schulinternen Verbesserungsprozesses ist das Konzept regelmäßig, beispielsweise alle zwei Jahre, auf Aktualität zu prüfen. Dabei können auch die Checklisten auf erneute Relevanz geprüft werden, wobei vormals mit „Nein“ angekreuzte Anforderungen relevant werden können.

Darüber hinaus kann die Schule an jeder Stelle des Basis-Informationssicherheitskonzeptes Anpassungen vornehmen, um das Konzept an die eigenen Bedürfnisse anzupassen. Auch die Überführung in ein schulinternes Layout oder in die Integration evtl. bereits existierender Konzepte ist möglich. Die Vorgaben der Schulen durch öffentliche Stellen bleiben dabei unberührt.

Für die Umsetzung des Basis-Informationssicherheitskonzeptes ist die Schulleitung der jeweiligen Schule verantwortlich. Sie kann die Umsetzung der resultierenden Aufgaben einzeln oder ganz delegieren.

Verwendete Vorgaben

Das Basis-Informationssicherheitskonzept berücksichtigt eine Vielzahl von Vorgaben, die durch die Schulen umzusetzen sind. Das vorliegende Konzept umfasst einige dieser Vorgaben. Die berücksichtigten Vorgaben sind folgend aufgelistet:

- BSI-Grundschutz-Kompendium Edition 2019;
- Praxishandbuch Schuldatenschutz des ULD Schleswig-Holstein, 2009;
- Dienstanweisung für die Nutzung der Schulverwaltungsrechner im Landesnetz Bildung (LanBSH) des MBWK, veröffentlicht am 03.07.2017;
- Themenpapier Internetnutzung in Schulen vom IQSH;
- IT Ausstattungsempfehlung 2015 des IQSH, August 2015;
- Internet/WLAN Bekanntmachung des IQSH, 2013;
- Themenpapier Medienentwicklungsplanung des IQSH, 2015;
- Bekanntmachung Schulische Nutzung von Cloud-Diensten des MBWK, 2013.

Es ist zu berücksichtigen, dass die inhaltlichen Anforderungen aus den zuvor aufgeführten Quellen in die Erstellung des Basis-Informationssicherheitskonzeptes nicht vollumfänglich einbezogen wurden. Das Konzept berücksichtigt ausschließlich für die Basisabsicherung relevanten Informationen und erhebt keinen Anspruch auf Vollständigkeit. Die Schulleitung kann aber selbstständig in der Nutzung des Basis-Informationssicherheitskonzeptes die Anforderungen aus den benannten und unbenannten Quellen ergänzen.

1. Verantwortlichkeiten und Ziele der Informationssicherheit

Verantwortlichkeiten der Schulleitung:

Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl analog auf Papier, digital in Computern oder in Aktenform gespeichert sein. Personenbezogene Daten unterliegen den Datenschutzgesetzen und stellen eine besondere Art schützenswerter Informationen dar. Für die Planungs-, Lenkungs- und Kontrollaufgabe, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit in der [Name der Schule] aufzubauen und kontinuierlich umzusetzen, ist die Schulleitung verantwortlich. Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.

Die Schulleitung ist dafür verantwortlich die Informationssicherheit und insbesondere den Datenschutz (laut § 2 SchulDSVO) in den Schulalltag zu integrieren und die zugehörigen technischen und organisatorischen Maßnahmen umzusetzen und zu kontrollieren. Somit ist die Schulleitung gegenüber möglichen Betroffenen, dafür verantwortlich, dass allen informationssicherheits- und datenschutzrechtlichen Vorschriften, Vorgaben und Notwendigkeiten Rechnung getragen wird. Um das zu gewährleisten müssen folgende Maßnahmen von der Schulleitung durchgeführt werden:

- Übernahme der Gesamtverantwortung für die Informationssicherheit in der [Name der Schule]. Sicherheitsprozess initiieren, Zuständigkeiten der Lehrkräfte und des Sekretariats sowie sämtlichen weiteren Schulpersonals für die Informationssicherheit festlegen;
- Sensibilisierung der Lehrkräfte und des Sekretariatspersonals sowie sämtlichen weiteren Schulpersonals für informationssicherheits- und datenschutzrechtliche Risiken und Gefährdungen. Dabei genügt es nicht, nur Anordnungen zur Informationssicherheit und des Datenschutzes zu erteilen, die Lehrkräfte und das Sekretariatspersonal sowie sämtliches weiteres Schulpersonal müssen ein Verständnis dafür entwickeln, aus welchen Gründen die Maßnahmen durchgeführt werden müssen. Insbesondere zur Sensibilisierung zum Thema Datenschutz sollte die Schulleitung dabei auf die Belehrung gem. Anlage 1 i.V.m. § 3 SchulDSVO zurückgreifen, die zusätzlich aktenkundig gemacht werden muss.

Die Schulleitung kann als Teil einer Aufgabendelegation gem. § 33 Abs. 6 SchulG Ihre Stellvertreterinnen oder Stellvertreter oder eine anderen Lehrkraft beauftragen, die Beachtung und Umsetzung der Informationssicherheit und des Datenschutzes in der [Name der Schule] zu überwachen. Die Letztverantwortung verbleibt auch dann bei der Schulleitung.

Verantwortlichkeiten der Lehrkräfte und der Sekretariatsmitarbeiter/-innen sowie sämtlicher weiterer Schulmitarbeiter/-innen:

Alle Lehrkräfte und das Sekretariatspersonal sowie sämtliches weiteres Schulpersonal der [Name der Schule] gewährleisten die Informationssicherheit durch verantwortungsbewusstes Handeln und halten die für die Informationssicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen ein. Sie gehen korrekt und verantwortungsvoll mit den von ihnen genutzten IT-Systemen, Daten und Informationen um.

In der folgenden Tabelle werden die Verantwortlichkeiten für die Umsetzung der Informationssicherheit und des Datenschutzes in der [Name der Schule] aufgeführt[1].

Verantwortlich für	Name, Vorname	Telefon	E-Mail-Adresse
Informationssicherheit			
Datenschutz			
Schlüsselverwaltung			
Zugangskontrolle			
Verwaltung IT-Ausstattung/ technische Geräte			
Benutzerrechte IT- Systeme			
Notfallverwaltung			
Gebäudesicherung			
Schulspezifische Verantwortlichkeiten:			

Tabelle 2: Verantwortlichkeiten der Informationssicherheit und des Datenschutzes

[1] Eine Zuordnung von einer Person zu mehreren Verantwortlichkeiten ist zulässig.

Ziele der Informationssicherheit:

Wie zuvor erwähnt hat die Informationssicherheit an Schulen den Schutz von Informationen als Ziel und ist somit integraler Bestandteil aller Schulverwaltungsprozesse. Durch die zunehmende Erhebung, Verarbeitung, Speicherung, Löschung und den Transport von Informationen mit Hilfe von IT-Systemen sind nachfolgende Schutzziele anzustreben:

1. Vertraulichkeit der Daten;
2. Integrität sämtlicher Daten und IT Systeme;
3. Verfügbarkeit sämtlicher Daten und IT-Systeme.

Vertraulichkeit bedeutet, dass Informationen nicht durch Unbefugte eingesehen oder genutzt werden können.

Integrität versichert die Vollständigkeit der Informationen sowie die Änderung durch ausschließlich befugte Personen.

Verfügbarkeit bedeutet, dass Informationen zum geforderten Zeitpunkt zur Verfügung stehen.

Um diese Schutzziele zu erreichen, müssen die Bedrohungen und Gefahren für die Informationssicherheit bekannt sein.

Beispiele für Gefahren:

• Verfügbarkeit Stromausfall, Festplattencrash, Wasserschaden, Brand etc.

• Vertraulichkeit: Zutritt zu Serverräumen, Geräten oder zu Datenträgern und Akten etc.

• Integrität: Programmabstürze, Viren.

In den folgenden Kapiteln werden wichtige Hinweise und Praxisanweisungen gegeben, um diese Ziele der Informationssicherheit an den Schulen mit ihrem besonderen Stellenwert zu berücksichtigen.

2. Umgang mit Informationen

2.1 Informationsklassen

Informationen müssen anhand ihres Schutzbedarfes geschützt werden. So gilt es bspw. personenbezogene Daten sicher verschlüsselt zu speichern und vor dem Zugriff Dritter zu schützen, währenddessen Einladungen zu Schulveranstaltungen öffentlich gemacht werden könnten. Um eine Bewertung darüber abgeben zu können, welchen Schutzbedarf eine Information besitzt, ist es notwendig eine allgemeine Klassifizierung der Informationen vorzunehmen.

Entsprechend der Klassifizierung müssen Daten und Dokumente geschützt werden, um den Zugriff von Dritten ausschließen zu können. Dafür definiert die [Name der Schule] folgende Informationsklassen:

- **Öffentlich zugänglich** – keine schützenswerten Daten;
- **Intern** – schützenswerten Daten;
- **Vertraulich** – besonders schützenswerte Daten.

Jedes Dokument, das nicht der Informationsklasse „Öffentlich zugänglich“ zugehörig ist, muss durch den Verfasser der Klasse „Intern“ oder „Vertraulich“ zugeordnet werden. Die Informationsklasse muss durch den Verfasser in dem jeweiligen Dokument mittig in der Kopfzeile gut sichtbar auf jeder Seite vermerkt werden.

Die folgende Tabelle gibt einen Überblick über die Informationsklassen und deren Schutzbedarf.

Klassifi-zierung	Beschreibung	Schutz-bedarf	Beispiele
Öffentlich zugänglich	Daten aus Informationsquellen, die geeignet und dazu bestimmt sind, der Allgemeinheit (d.h. einem individuell nicht bestimmbaren Personenkreis) Informationen zur Verfügung zu stellen (BVerfG, Beschluss vom 10. März 1993, 1 BvR 1192/92). Öffentlich zugänglich sind diese Quellen nur, wenn sie ohne Nachweis einer Berechtigung oder eines besonderen Interesses von allen genutzt werden können. Im Schulkontext kann unter öffentlich zugänglichen Daten sämtliche Informationen verstanden werden die beispielsweise auf der Schulhomepage der Schule veröffentlicht sind, insofern sie auch wirklich frei zugänglich sind.	Niedrig	Aushänge, Websites oder Flyer zu: • Ganztagsangeboten, • Schulordnungen, • Mittagessen, • Fördervereinen, • Schulprofilen, • Kooperationen, • Aktionen, • pädagogischen Konzepten, • Wahlpflichtkursen, • Öffentlichen Fotogalerien, • Terminen, • Elternbeiräten, • Kontaktdaten zu bspw. Schulsekretariat etc.

Klassifi-zierung	Beschreibung	Schutz-bedarf	Beispiele
Intern	Intern sind sämtliche Daten die innerhalb einer bestimmten Organisation zum Zwecke organisatorischer Abläufe in irgendeiner Weise verarbeitet werden. Im Schulkontext handelt es sich um Informationen die zur Verwaltung der [Name der Schule] bzw. der Schüler/-innen und Lehrkräfte benötigt werden.	Mittel	• Fächerdaten, • Stundenpläne, • Vertretungspläne, • Klassenbuch, • Raumpläne etc.
Vertraulich	Alle Daten, die nicht für die Öffentlichkeit bestimmt sind und einen hohen Schutzbedarf gem. Informationssicherheitsschutz und Datenschutzrecht haben.	Hoch	• Schülerstammdaten, • Elternstammdaten, • Lehrkräftestammdaten, • Schülerlaufbahndaten, • Schülerakten, • Zeugnisse, • besonders schützenswerte Daten (z.B. Gesundheitsdaten der Schüler, Konfession, Staatsangehörigkeit) etc.

Tabelle 3: Informationsklassen mit Beschreibung und Beispielen

2.2 Umgang mit Informationen

Die sichere Handhabung von Informationen ist ein zentraler Bestandteil der Informationssicherheit. Zur Schaffung einer angemessenen Informationssicherheit ist es notwendig, dass ein sicherer Umgang mit Informationen durch die Schulleitung, das Sekretariat und der Lehrkräfte sowie sämtlicher weiterer Schulmitarbeiter/-innen gewährleistet wird. Dazu sind allgemeine und übergreifende Anforderungen im Bereich der Organisation der [Name der Schule] notwendig, die Informationsflüsse, Prozesse, Rollenverteilung sowie die Aufbau- und Ablauforganisation regeln.

2.2.1 Umgang entsprechend der Informationsklassen

Informationen sind entsprechend ihres Schutzbedarfes abzusichern. Daher gibt es beim Umgang mit klassifizierten Dokumenten sicherheitsrelevante Anforderungen. Die folgende Tabelle beschreibt die Anforderungen entsprechend der Informationsklassifizierungen. Diese Vorgaben sind von allen Mitarbeiterinnen und Mitarbeitern zu berücksichtigen und im Tagesgeschäft umzusetzen.

Klassifi-zierung	Schutz-bedarf	Absicherung	Beispiele
Öffentlich zugänglich	Niedrig	Die Informationen haben keine Anforderungen in Bezug auf die Informationssicherheit und können bzw. müssen offen ausliegen.	• Aushänge • Flyer & Handreichungen • Hausordnungen
Intern	Mittel	Dokumente sind unter Aufsicht zu übermitteln, dürfen nicht offen liegen und sind nach der Nutzung angemessen zu verwahren, sodass Dritte darin keine Einsicht nehmen können.	• Klassenbuch wird durch Lehrer am Ende des Schultages im geschlossenen Lehrerzimmer aufbewahrt
Vertraulich	Hoch	Der Zugriff auf die Informationen ist nur einem bestimmten Mitarbeiterkreis gestattet und mit entsprechenden Maßnahmen abgesichert. Dokumente werden verschlossen aufbewahrt. Daten auf Datenträgern sind zu verschlüsseln.	• Schülerakte ist im Sekretariat in verschlossenen Schränken aufzubewahren • Datenträger mit Noten und Zeugnissen sind verschlüsselt

Tabelle 4: Informationsklassen und deren Schutzbedarf

2.2.2 Weitere Maßnahmen zum Umgang mit Informationen

Die Durchführung der folgenden Maßnahmen dient der Erreichung einer Basisabsicherung und sind entsprechend ihrer Anwendbarkeit in der [Name der Schule] umzusetzen:

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1	Der aufgeräumte Arbeitsplatz	Das Personal des Sekretariats, Lehrkräfte und weiteres Personal der [Name der Schule] wird darauf hingewiesen, dass an unbeaufsichtigten Arbeitsplätzen weder sensible Informationen noch IT-Systeme frei zugänglich sein dürfen. Die Arbeitsplätze des Sekretariatspersonals und der Lehrkräfte sowie des weiteren Schulpersonals werden stichprobenartig durch die Schulleitung kontrolliert, ob auf schutzbedürftige Informationen offen zugegriffen werden kann.	☐ Ja ☐ Nein

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
2	Dokumente der Schulverwaltung	Die Dokumente der Schulverwaltung müssen gem. § 7 SchulDSVO geführt werden und dürfen nur von dem Sekretariatspersonal und Lehrkräften sowie weiterem Schulpersonal der [Name der Schule] eingesehen werden, soweit sie diese für ihre Aufgabenerfüllung benötigen. In die Schülerakte werden nur die Dokumente aufgenommen die in § 7 Abs.1 SchulDSVO aufgeführt sind. Gesondert von der Schülerakte zu führen sind beispielsweise Krankmeldungen, die sonderpädagogische Schülerakte gem. § 7 Abs. 2 SchulDSVO, Klassenarbeiten, sowie Zweit- und Durchschriften von Zeugnissen.	☐ Ja ☐ Nein
3	Regelung der Vorgehensweise für die Löschung und Vernichtung von Informationen	Die Löschung und Vernichtung von Informationen und Dokumenten ist detailliert in §10 SchulDSVO geregelt und wird in der [Name der Schule] entsprechend umgesetzt. Hierbei kann es sich sowohl um elektronisch gespeicherte Dokumente handeln als auch um Dokumente die in Papierform in Akten aufbewahrt werden. Die Schulleitung trägt die Verantwortung dafür, dass diese Löschfristen, eingehalten werden, um die Datenschutzkonformität zu gewährleisten.	☐ Ja ☐ Nein
4	Löschen von Datenträger vor und nach dem Austausch	Werden schützenswerte Informationen auf schon vorher benutzten Datenträgern übergeben, dann müssen alle darauf befindlichen Daten sicher gelöscht werden.	☐ Ja ☐ Nein
5	Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern	Dem Sekretariatspersonal und den Lehrkräften sowie dem weiteren Schulpersonal werden für das Löschen und Vernichten geeignete Verfahren vorgegeben. So sollte es für verschiedene Datenträgerarten immer geeignete Geräte und Werkzeuge geben, mit denen Sekretariatsmitarbeiter/-innen und Lehrkräfte die gespeicherten Informationen löschen oder vernichten können.	☐ Ja ☐ Nein
6	Geregelte Außerbetrieb-nahme von IT-Systemen und Datenträgern	In der [Name der Schule] sollte ein Sekretariatsmitarbeiter/-in, Lehrkraft oder Schulmitarbeiter/-in ausgewählt werden der/die verantwortlich für die IT- Ausstattung ist. Diese Person muss regeln und dokumentieren, wie IT-Systeme und Datenträger außer Betrieb zu nehmen sind. Dabei ist sicherzustellen, dass vor den Außerbetriebnahmen alle auf einem IT-System oder Datenträger gespeicherten Informationen sicher gelöscht sind.	☐ Ja ☐ Nein

Tabelle 4: Maßnahmen zum Umgang mit Informationen

2.3 Personenbezogene Daten und Datenverarbeitung

Nach den Definitionen der Richtlinie EU 2016/679 (EU-DSGVO) und des Bundesdatenschutzgesetzes (BDSG) sind personenbezogene Daten all jene Informationen, die sich auf eine natürliche Person beziehen oder zumindest beziehbar sind und so Rückschlüsse auf deren Persönlichkeit ermöglichen. Besondere Kategorien von personenbezogenen Daten sind im Artikel 9 EU-DSGVO aufgeführt. Hierbei handelt es sich beispielsweise um Informationen über die ethnische und kulturelle Herkunft, politische, religiöse und weltanschauliche Überzeugungen, Gesundheit, Sexualität und Gewerkschaftszugehörigkeit. Sie sind besonders schützenswert.

Im Schulkontext sprechen wir hier über alle Informationen der Schülerinnen und Schüler, der Lehrkräfte, des Sekretariatspersonals und des Schulpersonals der [Name der Schule] die bei Schulverwaltungsprozessen verarbeitet werden. Unter Datenverarbeitung verstehen sich dabei die folgenden **Verarbeitungsschritte**:

1. **Erheben**: Hiermit wird das (aktive) Beschaffen von Daten umschrieben. In der Schule erfolgt das bspw. durch den ausgefüllten Schüleranmeldebogen oder durch den ausgefüllten Aufnahmebogen einer neuen Lehrkraft, Sekretariatsmitarbeiter/-in oder Schulmitarbeiter/-in.
2. **Speichern**: Damit ist das Aufbewahren von Daten auf Datenträgern oder in Dateisystemen gemeint. Datenträger ist ein umfassender Begriff, der – wie auch der Begriff „Speichern" – in erster Linie immer mit der elektronischen Datenverarbeitung (EDV) in Zusammenhang gebracht wird. Er beschränkt sich aber nicht darauf! Unter Datenträgern versteht man beispielsweise: Papier, Festplatten, Disketten, CD-ROM, DVD, Streamer-Tapes (also Aufzeichnungsbänder von Bandlaufwerken) und USB-Sticks. Im Schulkontext ist hier besonders hervorzuheben, dass Datenträger nicht nur in elektronischer Form auftreten, sondern dass damit auch sämtliche Dokumente und Unterlagen gemeint sind, die in Papierform in Akten verwaltet werden (manuelle Dateisysteme).
3. **Übermitteln**: Darunter versteht man die Weitergabe von Daten an Dritte (natürliche oder juristische Personen, öffentliche oder nichtöffentliche Stellen). Die Übermittlung von Daten kann dabei in jeder Kommunikationsform geschehen. Es ist unerheblich, ob die Informationen im Gespräch (also von Angesicht zu Angesicht oder per Telefon), per Brief, per Fax, mittels E-Mail oder elektronischen Abruf weitergegeben werden. Im Schulkontext muss die Schulleitung dem Sekretariatspersonal, Lehrkräften und Schulpersonal deutlich machen, dass auch in einem persönlichen Gespräch untereinander nicht sämtliche personenbezogene Daten der Schülerinnen und Schüler verbreitet werden dürfen. Darüber hinaus müssen bei der Kommunikation mit externen Datenempfängern sichere Kommunikationswege ausgewählt werden, beispielsweise bei der Übermittlung von personenbezogenen Daten per E-Mail oder an das statistische Landesamt.
4. **Sperren**: Hierunter versteht man, dass gespeicherte Daten grundsätzlich nicht mehr weiterverarbeitet (also beispielsweise genutzt oder übermittelt) werden dürfen. Dies trifft zu, wenn Daten für den ursprünglichen Zweck nicht mehr benötigt werden, aber wegen vorgeschriebener Aufbewahrungsfristen noch nicht gelöscht werden dürfen. In der Schule sind davon sämtliche Schülerdokumente von abgegangenen bzw. entlassenen

Schülerinnen und Schülern betroffen. Diese Daten werden nicht mehr weiterarbeitet, sie dürfen aber aufgrund von Aufbewahrungsfristen nicht gelöscht werden.

5. **Löschen**: Das Landesdatenschutzgesetz spricht hier vom Unkenntlich machen gespeicherter Daten. Gemeint ist damit das unwiederbringliche Vernichten von Informationen. Auch in diesem Fall wird der Begriff automatisch mit EDV in Verbindung gebracht. Im Schulkontext ist hier nicht nur die Löschung von Daten in elektronischer Form in Betracht zu ziehen, sondern auch das Vernichten sämtlicher Dokumente und Unterlagen, die in Papierform in Akten abgelegt worden sind.

Die Eltern und Schüler/-innen der [Name der Schule] haben das Recht auf informationelle Selbstbestimmung, das bedeutet das nur die Daten in der Schulverwaltung aufgenommen werden dürfen die gem. Anlage 2 zu § 5 SchulDSVO legitimiert wurden. Die weitere Verarbeitung von zusätzlichen personenbezogenen Daten ist nur mit Einwilligung der Eltern zulässig. Diese kann beispielsweise im Schüleranmeldebogen für die Verarbeitung eines Lichtbilds für Schulverwaltungszwecke, zur Darstellung von Bildern/Videos auf der Schulhomepage oder zur Erstellung einer Klassenliste eingeholt werden.

3. Allgemeine Informationssicherheit

3.1 Gebäudezutritt

Das Schulgebäude der [Name der Schule] bildet den physischen Rahmen in dem die Schulverwaltungsprozesse, der IT-Betrieb, die Lehre und die pädagogische Betreuung der Schüler/-innen stattfinden. Das Schulgebäude kann sowohl von schulinternen Personen (z.B. Schulleitung, Lehrkräfte, Sekretariatspersonal und Schüler/-innen) als auch von schulfremden Parteien (z.B. Eltern, Reinigungspersonal, Lieferanten etc.) betreten werden. Aus diesem Grund ergeben sich auch unterschiedliche Sicherheitsansprüche an den Schulgebäudezutritt. Während der Schulzeit muss den schulinternen Personen ein schneller und praktikabler Zutritt zum Schulgebäude möglich sein, gleichzeitig dürfen aber schulfremde oder unbefugte Personen keinen unkontrollierten Zutritt zum Schulgebäude haben.

Wenn Unbefugte in das Schulgebäude gelangen, kann das verschiedene andere Sicherheitsgefährdungen nach sich ziehen. Unbefugte Personen können durch vorsätzliche Handlungen wie beispielsweise Diebstahl oder Manipulation von Informationen oder IT-Systemen, aber auch durch unbeabsichtigtes Fehlverhalten (z. B. aufgrund mangelnder Fachkenntnisse) Schäden verursachen.

In der folgenden Tabelle werden die Anforderungen beschrieben, um den Zutritt von schulinternen und schulfremden Personen in das Schulgebäude der [Name der Schule] zu reglementieren.

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1	Verantwortlich-keiten	Es wurde ein Verantwortlicher für die Zutrittskontrolle in das Schulgebäude bestimmt.	☐ Ja ☐ Nein
2	Zutrittsregelung und -kontrolle	Der Zutritt zum Schulgebäude wird geregelt und kontrolliert. Die Schulleitung (ggf. der Verantwortliche für die Zutrittskontrolle) hat ein Konzept für die Zutrittskontrolle der einzelnen Schutzbereiche des Schulgebäudes erstellt (siehe auch 3.2). Die Zahl der zutrittsberechtigten Personen ist auf ein Mindestmaß reduziert. Schulfremde Personen erhalten Zutritt zum Schulgebäude, wenn eine vorherige Prüfung (idealerweise durch den Verantwortlichen für die Zutrittskontrollen) der Notwendigkeit des Zutritts vorgenommen wurde. Alle erteilten Zutrittsberechtigungen werden von dem Verantwortlichen für die Zutrittskontrolle oder durch die Schulleitung bzw. das Schulsekretariatspersonal dokumentiert und regelmäßig auf ihre Wirksamkeit überprüft.	☐ Ja ☐ Nein

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
3	Geschlossene Fenster und Türen	Fenster und nach außen öffnende Türen (Balkone, Terrassen) des Schulgebäudes werden in Zeiten, in denen ein Raum nicht besetzt ist, geschlossen. Die Schulleitung gibt eine entsprechende Anweisung an das schulinterne Personal und prüft regelmäßig, ob die Anweisung eingehalten wird.	☐ Ja ☐ Nein
4	Abgeschlossene Türen	Das schulinterne Personal ist von der Schulleitung angewiesen, die öffentlichen Zugänge des Schulgebäudes zu verschließen. Es wird sporadisch überprüft, ob das umgesetzt wird. Im Schulalltag könnte sich diese Vorgabe aus unterschiedlichen Gründen als nicht praktikabel erweisen. Aus diesem Grund wären die folgenden Optionen denkbar: Option 1: Die öffentlichen Zugänge des Schulgebäudes werden nur außerhalb der Schulzeiten verschlossen, während der Schulzeit bleiben sie geöffnet. Option 2: Die öffentlichen Zugänge des Schulgebäudes werden nur außerhalb der Schulzeiten verschlossen, während der Schulzeit findet eine Zugangskontrolle durch schulinternes Personal statt. Option 3: Die öffentlichen Zugänge des Schulgebäudes bleiben durchgängig verschlossen. Das schulinterne Personal sowie alle Schüler/-innen haben eine eigene Zugangskarte oder haben Kenntnis über den Türzugangs-PIN. Option 4: Schulspezifische Zugangslösung: [Beschreiben Sie bitte hier die schulspezifische Zugangslösung]	☐ Ja ☐ Nein ☐ Ja ☐ Nein ☐ Ja ☐ Nein ☐ Ja ☐ Nein ☐ Ja ☐ Nein
5	Schlüssel-verwaltung	Für alle Schlüssel des Schulgebäudes der [Name der Schule] wird von dem Verantwortlichen für die Zutrittskontrolle oder von der Schulleitung ein Schließplan erstellt. Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln zum Schulgebäude werden zentral geregelt (idealerweise bei dem Verantwortlichen für die Zutrittskontrollen). Reserveschlüssel werden vorgehalten und gesichert, sind aber für Notfälle griffbereit aufzubewahren (idealerweise bei dem Verantwortlichen für die Zutrittskontrollen). Nicht ausgegebene Schlüssel werden	☐ Ja ☐ Nein

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
		sicher aufbewahrt. Jede Schlüsselausgabe zum Schulgebäude wird dokumentiert.	
6	Alarmanlagen und zusätzliche Schlösser	Sämtliche öffentliche und nicht öffentliche Zugänge, Fenster und Türen zum Schulgebäude der [Name der Schule] werden mit zusätzlichen Sicherungsmaßnahmen beispielsweise die Installation von Alarmanlagen und zusätzlichen Schlössern ausgestattet.	☐ Ja ☐ Nein

Tabelle 5: Anforderungen zur Absicherung des Schulgebäudezutritts

3.2 Räume im Schulgebäude

Die Räume im Schulgebäude der [Name der Schule] können in öffentliche, eingeschränkte und gesperrte Räume eingeteilt werden und werden in der nachfolgenden Tabelle kurz erläutert:

Raumkategorie	Beschreibung	Beispiele
Öffentlich	Öffentliche Räume sind für schulinterne und schulfremde Personen ohne Einschränkungen zugänglich.	Schulfoyer, Turnhalle, Aula, Unterrichtsraum
Eingeschränkt	Eingeschränkte Räume sind nur für einen bestimmten schulinternen Personenkreis zugänglich.	Sekretariat, Lehrerzimmer etc.
Gesperrt	Gesperrte Räume sind nur für befugte Personen zugänglich, die einer umfangreichen Überprüfung unterzogen werden muss.	Schulleiterraum, Serverräume, Heizungsräume, Aktenaufbewahrung etc.

Tabelle 6: Beschreibung der Raumkategorien

Alle Räume der [Name der Schule] inklusive für Schulzwecke genutzte Räume im häuslichen Umfeld oder unterwegs, in denen schutzbedürftige Informationen (insbesondere der Schüler/-innen) aufbewahrt bzw. weiterverarbeitet werden, müssen vor dem unbefugten Zutritt von Dritten geschützt werden. Unbefugte Personen können in solchen Räumen durch vorsätzliche Handlungen (Manipulationen oder Vandalismus), aber auch durch unbeabsichtigtes Fehlverhalten (aufgrund mangelnder Fachkenntnisse) Schäden verursachen. Durch Eindringlinge könnten beispielsweise Passwörter zurückgesetzt oder direkt auf die Server zugegriffen werden. Außerdem könnten sie sensible Informationen der schulinternen Personen insbesondere der Schüler/-innen (z.B. sonderpädagogische Schülerakte, Gesundheitsdaten etc.) auf Papier oder Datenträgern entwenden oder verändern.

Manipulationen können vom falschen Erfassen von Daten, Änderungen von Zugriffsrechten bis hin zur Manipulation von Betriebssystemen, Datenträgern oder IT-Systemen reichen. Die Angriffe sind umso wirkungsvoller, je später sie entdeckt werden, je umfassender die Kenntnisse des Täters und je tiefgreifender die Folgen für einen Arbeitsvorgang sind.

In der folgenden Tabelle werden die Anforderungen beschrieben, die eine Sicherung der Räume in der [Name der Schule] gewährleisten soll.

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1	Beaufsichtigung oder Begleitung von Fremdpersonen	Die Schulleitung, Lehrkräfte und das Sekretariatspersonal werden dazu angehalten, schulfremde Personen nicht unbeaufsichtigt zu lassen.	☐ Ja ☐ Nein
2	Sicherung von Serverräumen	Für die Serverräume werden angemessene technische und organisatorische Vorgaben durch die Schulleitung definiert und umgesetzt. Versorgungsleitungen (z. B. für Wasser oder Gas) verlaufen möglichst nicht in unmittelbarer Nähe von schutzbedürftigen Technikkomponenten des Serverraums. Vorhandene Versorgungsleitungen müssen zumindest an den kritischen Stellen regelmäßig überprüft werden, ob sie noch dicht sind.	☐ Ja ☐ Nein
3	Auswahl und Nutzung des Sekretariats, Arbeitsplätze der Lehrkräfte, Räumlichkeiten der Schulleitung	Es werden nur geeignete Räume als Sekretariat, Arbeitsplätze der Lehrkräfte oder Räumlichkeiten der Schulleitung genutzt. Auch sind diese Räumlichkeiten für den Schutzbedarf bzw. das Schutzniveau der dort verarbeiteten Informationen angemessen ausgewählt und ausgestattet. Anforderung 1: Das Sekretariat liegt in einem sicherheitsrelevanten Bereich. ODER: Das Sekretariat liegt aufgrund von Publikumsverkehr in einem nicht sicherheitsrelevanten Bereich, aber das Schutzniveau der Informationen ist gewährleistet. Anforderung 2: Die Arbeitsplätze der Lehrkräfte liegen in Räumlichkeiten mit eingeschränktem Zugang. Anforderung 3: Die Räumlichkeiten der Schulleitung liegen in einem gesperrten hoch sicherheitsrelevanten Bereich des Schulgebäudes. Anforderung 4: Schulspezifische Raumverteilung	☐ Ja ☐ Nein ☐ Ja ☐ Nein ☐ Ja ☐ Nein ☐ Ja ☐ Nein ☐ Ja ☐ Nein
5	Geschlossene Fenster und Türen	Wenn die Schulleitung, das Sekretariatspersonal oder die Lehrkräfte die Räumlichkeiten verlassen an denen schutzbedürftige Informationen	☐ Ja

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
		verarbeitet werden, dann werden alle Fenster geschlossen. Zusätzlich werden bei Verlassen dieser Räumlichkeiten die Türen abgeschlossen. Dies betrifft insbesondere Sekretariate, Schulleiterzimmer, Archive etc.	☐ Nein
6	Aufgeräumter Arbeitsplatz	Das Sekretariatspersonal und die Lehrkräfte der [Name der Schule] sind darauf hingewiesen worden, dass an unbeaufsichtigten Arbeitsplätzen weder sensible Informationen noch IT-Systeme frei zugänglich sein dürfen. Die Arbeitsplätze des Sekretariatspersonals und Lehrkräfte werden stichprobenartig durch die Schulleitung kontrolliert werden, ob auf schutzbedürftige Informationen offen zugegriffen werden kann.	☐ Ja ☐ Nein
7	Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger	Das Sekretariatspersonal und die Lehrkräfte haben durch die Schulleitung eine Anweisung erhalten, vertrauliche Dokumente und Datenträger verschlossen aufzubewahren, wenn sie nicht verwendet werden. Dafür sind geeignete Behältnisse (z.B. Schränke, Schubläden etc.) in den Büroräumen oder in deren Umfeld aufgestellt werden.	☐ Ja ☐ Nein

Tabelle 7: Maßnahmen zur Sicherung der Schulräume

3.3 Überwachung von Tresoren

Tresore in der [Name der Schule] werden verwendet, um besonders schützenswerte Dokumente, Datenträger, Gegenstände, Wertsachen etc. vor Datenmissbrauch und Diebstahl zu schützen.

Bei der Verwendung von Tresoren muss zunächst einmal festgelegt werden, in welchen Räumen des Schulgebäudes diese stehen sollen und wie sie nicht sichtbar aufgestellt werden können. Dazu empfiehlt es sich Tresore in hoch sicherheitsrelevanten und gesperrten Bereichen des Schulgebäudes zu platzieren z.B. im Raum des Schulleiters. Um den Zugang zum Tresorinhalt zu kontrollieren, sollte festgelegt werden, wer die Tresorschlüssel verwaltet und dementsprechend auch dafür verantwortlich ist, dass keine unbefugte Personen Zugang zum Tresorinhalt erhalten. Voraussetzung dafür ist, dass die Schulleitung zunächst einmal festlegt, wer den Tresor überhaupt öffnen darf. Dabei ist es wichtig auch Vertretungsregelungen im Krankheitsfall anzuordnen, um den Tresor jederzeit öffnen zu können. Der Verantwortliche der Schlüsselhoheit sollte lückenlos dokumentieren, welche Personen Zugang zum Tresorinhalt hatten und zu welchem Zeitpunkt der Tresor geöffnet hat.

Darüber hinaus sollte von der Schulleitung generell geregelt werden, welche Dokumente, Datenträger oder Gegenstände einen hohen Schutzbedarf besitzen und somit im Tresor eingeschlossen werden sollten.

Zur Absicherung der Tresore in der Schule sind folgende Maßnahmen empfehlenswert:

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1	Gesperrte Räumlichkeiten	Der Tresor befindet sich in einer gesperrten Räumlichkeit des Schulgebäudes.	☐ Ja ☐ Nein
2	Nicht-Sichtbarkeit	Der Tresor ist nicht sichtbar im Raum aufgestellt, sodass er von Dritten nicht direkt gesehen bzw. als solches erkannt werden kann.	☐ Ja ☐ Nein
3	Schlüsselverwaltung festlegen	Die Schlüsselverwaltung für den Tresor wird zentral von einer verantwortlichen schulinternen Person durchgeführt.	☐ Ja ☐ Nein
4	Zugriffsberechtigungen	Die Schulleitung hat in Abstimmung mit den Verantwortlichen der Schlüsselverwaltung festgelegt, wer Zugriff auf den Tresorinhalt erhalten darf.	☐ Ja ☐ Nein
5	Dokumentation des Zugriffs	Die verantwortliche Person für die Schlüsselverwaltung dokumentiert wer Zugriff auf den Tresorinhalt hatte und wann der Zugriff erfolgt ist.	☐ Ja ☐ Nein
6	Festlegung des Tresorinhalts	Die Schulleitung hat festgelegt, welche Dokumente, Datenträger und Gegenstände im Tresor eingeschlossen werden sollen.	☐ Ja ☐ Nein
7	Befestigung	Der Tresor ist fest verankert und befindet sich nicht in Fensternähe	☐ Ja ☐ Nein
8	Optional: Versicherung	Es wurde eine separate Versicherung mit ausreichenden Versicherungssummen für den Tresorinhalt abgeschlossen.	☐ Ja ☐ Nein

Tabelle 8: Maßnahmen zur Absicherung der Tresore

3.4 Notfallvorsorge

Generell ist ein Notfall ein (unvorhersehbares) Schadensereignis, bei dem wesentliche Prozesse oder Ressourcen einer Institution nicht wie vorgesehen funktionieren. Notfälle zeichnen sich dadurch aus, dass die Verfügbarkeit der entsprechenden Prozesse oder Ressourcen innerhalb einer geforderten Zeit nicht wiederhergestellt werden kann und der Geschäftsbetrieb stark beeinträchtigt ist. Im Schulkontext können wir die folgenden Notfälle identifizieren:

- Erheblicher Personalausfall (z.B. Sekretariatspersonal, Lehrkräfte etc.)
- Fehlerhafte/ nicht funktionierende Schulverwaltungssoftware,
- Verlust von schutzbedürftigen Daten (z.B. Verlust von Datenträgern, Akten etc.)
- Feuer im Schulgebäude

Die Notfallmaßnahmen umfassen eine Planung von Präventivmaßnahmen die zum einen Notfälle vermeiden und zum anderen sicherstellen sollen, dass in Notfällen zumindest die wichtigsten Schulprozesse möglichst unbeeinträchtigt weiter funktionieren können.

Die folgende Tabelle beinhaltet die Notfallmaßnahmen, die für die [Name der Schule] umgesetzt werden könnten:

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1	Festlegung von Verantwortlichkeiten	Die Schulleitung hat einen Notfallverantwortlichen ernannt, der die Gesamtverantwortung für die Umsetzung der Notfallmaßnahmen übernimmt.	☐ Ja ☐ Nein
2	Regelmäßige Datensicherung	Zur Vermeidung von Datenverlusten werden regelmäßige Datensicherungen durchgeführt.	☐ Ja ☐ Nein
3	Datensicherung des Notfallverantwortlichen	Der Notfallverantwortliche stellt sicher, dass sowohl die elektronischen Daten in den Schulverwaltungssystemen als auch die Daten, die in Papierform in den Akten abgelegt sind regelmäßig gesichert werden.	☐ Ja ☐ Nein
4	Sicherung mobiler Datenräger	Es werden regelmäßige Sicherheitskopien von Daten auf mobilen Datenträgern (z.B. USB-Sticks) erstellt. Es werden keine privaten Wechseldatenträger gesichert.	☐ Ja ☐ Nein
5	Sicherung von Daten in Papierform	Von wichtigen Dokumenten werden Kopien erstellt und räumlich getrennt von den Ursprungsdokumenten aufbewahrt.	☐ Ja ☐ Nein
6	Systemabsicherung	Mechanismen der automatischen Datensicherungen werden in den	☐ Ja

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
		Schulverwaltungssystemen durch regelmäßige Systemupdates sichergestellt (ggf. kann durch Dienstleister erfolgen).	☐ Nein
7	Dokumentation der Datensicherung	Der Notfallverantwortliche dokumentiert die erstellten Sicherungen (Datum, Art der Durchführung der Sicherung sowie gewählte Parameter, Beschriftung der Datenträger), sodass das Alter der Sicherungen nachvollziehbar ist.	☐ Ja ☐ Nein
8	Datensicherung testen	Der Notfallverantwortliche testet regelmäßig die ordnungsgemäße Funktionalität der Datensicherungen und stellt sicher, dass Sicherungen von Daten problemlos zurückgespielt werden können.	☐ Ja ☐ Nein
9	Aufbewahrung von Backup-Datenträgern	Backup-Datenträger sind mit Hilfe von verschließbaren Schränken vor unbefugtem Zugriff zu schützen. Die Backup-Datenträger werden räumlich getrennt von den Herkunftssystemen aufbewahrt. Der Aufbewahrungsort von Backup-Datenträgern erfüllt neben den geforderten Zugriffsmöglichkeiten auch die klimatischen (z.B. Hitze, Kälte, Wasser etc.) Bedingungen für eine längerfristige Aufbewahrung von Datenträgern?	☐ Ja ☐ Nein ☐ Ja ☐ Nein ☐ Ja ☐ Nein
10	Softwareausfall/ -störung	Bei Störungen oder Ausfall der Schulverwaltungssoftware wird der Notfallverantwortliche des IQSH kontaktiert. Ggf. Ansprechpartner IQSH einfügen.	☐ Ja ☐ Nein
11	Hardwareausfall/ -störung	Bei Störungen oder Ausfall der Schulverwaltungssoftware wird der entsprechende Dienstleister kontaktiert. Ggf. Ansprechpartner Dienstleister einfügen.	☐ Ja ☐ Nein

Tabelle 9: Maßnahmen zur Notfallvorsorge

3.5 Aktenaufbewahrung

Die Verwaltung von Dokumenten, Daten und Informationen an einem Aktenaufbewahrungsort der [Name der Schule] muss einen hohen Stellenwert in den Schulverwaltungsprozessen besitzen. Die Archivierung muss einerseits die Dokumente, Daten und Informationen bis zum Ablauf einer vorgegebenen Aufbewahrungsfrist (=Löschfrist) verfügbar halten, andererseits soll ihre Vertraulichkeit und Integrität bewahrt bleiben.

In der Schule sind davon Dokumente, Daten und Informationen betroffen, die sowohl elektronisch in der Schulverwaltungssoftware gespeichert werden als auch in Papierform in Akten oder Karteien aufbewahrt werden.

Für die konventionelle Speicherung (Akten und Karteien) sind folgende Aspekte zu berücksichtigen:

- Jede Schule hat ihre eigene Aktenorganisation. Überwiegend sind die Unterlagen über die Schülerinnen und Schüler in einzelnen Vorgängen zusammengeheftet sind. Diese Vorgänge bestehen in der Regel aus dem Schüleraufnahmebogen, den Durchschriften der Zeugnisse sowie weiterem Schriftwechsel, ggf. mit anderen Behörden oder den Eltern der Schülerinnen und Schüler. Die Schule ist nach den allgemeinen Maßnahmen zur Datensicherung gem. LDSG verpflichtet, diese Unterlagen vor dem Zugriff Unbefugter zu sichern.
- Um diese Vorgabe zu erfüllen, müssen die Unterlagen in abschließbaren Schränken aufbewahrt werden, die nach Dienstschluss verschlossen werden. Daneben legt der § 6 SchulDSVO fest, wer Zugang zum Datenbestand in der Schule und damit zu den Schülerakten (aber auch zu den elektronischen Datenbeständen) haben darf. Nur diejenigen Lehrkräfte dürfen von den Inhalten der Schülerakten Kenntnis nehmen, die diese Schülerinnen und Schüler auch unterrichten.

Für den Fall, dass schützenwerte Daten von Schülerinnen, Schülern und Eltern mit Hilfe von elektronischer Datenverarbeitung stattfinden, gelten für die Zugriffsrechte grundsätzlich dieselben Regelungen wie für Akten. Folgende Maßnahmen sollten bei der Verwendung einer Schulverwaltungssoftware (automatisiertes Verfahren) beachtet werden:

- Die Daten der Schülerinnen und Schüler und deren Eltern müssen vor dem Zugriff Unbefugter geschützt werden. Dafür sind Sicherheitsvorkehrungen in technischer wie auch in organisatorischer Hinsicht (schriftliche Regelungen) zu treffen.

- Die Aufbewahrungsfristen der einzelnen Dokumente die entweder elektronisch oder konventionell in Papierform in Akten gespeichert oder abgelegt werden sind in §10 SchulDSVO aufgeführt. Diese Vorschrift legt fest, welche Daten für welche Zeiträume zu speichern sind. Dabei handelt es sich um Höchstfristen. Die Fristen beginnen mit Ablauf des Schuljahres, in dem die Unterlagen und Dateisysteme jeweils erstellt bzw. geschlossen wurden. Alle übrigen schützenswerten Daten sind zu löschen, sobald sie für die konkrete Aufgabenerfüllung nicht mehr erforderlich sind, spätestens aber fünf Jahre nach Ablauf des Schuljahres, in dem der Vorgang geschlossen worden ist. Darüber hinaus ist zu beachten, dass die Dokumente vor

Löschung oder Vernichtung nach der Aufbewahrungsfrist einem Archiv zur Übernahme anzubieten sind (§ 10 Abs. 2 SchulDSVO).

- Die differenzierten Aufbewahrungsfristen machen es erforderlich, die Schülerakten von vornherein so zu organisieren, dass den Vorgaben der genannten Vorschrift gefolgt werden kann. In den Schülerakten dürfen neben dem Schüleraufnahmebogen auch die Kopien der Zeugnisse usw. gespeichert werden. Diese Unterlagen haben bereits unterschiedliche Aufbewahrungsfristen. Während Zeugnisdurchschriften 10 Jahre aufbewahrt werden dürfen, sind die Schülerakten lediglich zwei Jahre zu speichern. Um eine vorschriftsgemäße Vernichtung dieser Vorgänge zu erleichtern, sollten die Akten deshalb dementsprechend organisiert sein.

In der folgenden Tabelle werden mögliche Maßnahmen für eine effiziente Aktenaufbewahrung dargestellt.

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1	Organisation	Die Dokumente sind in elektronischer und in Papierform so abgelegt, dass die Löschfristen der einzelnen Dokumente einfach berücksichtigt werden können.	☐ Ja ☐ Nein
2	Öffentliche Archive	Die zu löschende Dokumente werden den öffentlichen Archiven zur Übernahme angeboten.	☐ Ja ☐ Nein
3	Löschfristen	Die Löschfristen der einzelnen elektronisch gespeicherten Dokumente werden gem. § 10 SchulDSVO ausgeführt bzw. die Dokumente in Papierform vernichtet.	☐ Ja ☐ Nein
4	Zugangskontrolle	Der Zutritt zu den Aktenaufbewahrungsorten ist geregelt und kontrolliert. Die Schulleitung (ggf. der Verantwortliche für die Zutrittskontrolle) hat ein Konzept für die Zutrittskontrolle der Schularchive erstellt. Die Zahl der zutrittsberechtigten Personen wird auf ein Mindestmaß reduziert. Alle erteilten Zutrittsberechtigungen werden bei der Schulleitung und dem Schulsekretariat dokumentiert und regelmäßig auf ihre Wirksamkeit überprüft. Das gilt sowohl für die Räume, in denen die Akten in Papierform in Schränken aufbewahrt werden als auch für die Räume in denen die Server für die elektronische Datenverarbeitung betrieben werden.	☐ Ja ☐ Nein
5	Aktenaufbewahrung	Dokumente, die in Papierform in Akten verwaltet werden, sind in verschließbaren Aktenschränken abgelegt.	☐ Ja ☐ Nein

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
6	Benutzerrechte	Bei Verwendung einer Schulverwaltungssoftware sind die korrekten Benutzerrechte hinterlegt.	☐ Ja ☐ Nein
7	Konsistente Indizierung der Dokumente	Alle in der Schulaufbewahrung abgelegten Dokumente werden eindeutig identifiziert abgelegt, um bei späteren Suchanfragen der Schülerinnen und Schüler die gewünschten Dokumente schnell wiederfinden zu können.	☐ Ja ☐ Nein
8	Regelmäßige Datensicherung	Bei digitalen Schulaufbewahrungen werden regelmäßige Datensicherungen durchgeführt (Datensicherungskonzept).	☐ Ja ☐ Nein

Tabelle 10: Maßnahmen zur effizienten Aktenaufbewahrung

3.6 Identifikation und Behandlung sicherheitsrelevanter Ereignisse

Als sicherheitsrelevantes Ereignis wird allgemein ein Ereignis bezeichnet, das sich auf die Informationssicherheit auswirkt und die Vertraulichkeit, Integrität und Verfügbarkeit beeinträchtigen. In der [Name der Schule] kann so ein sicherheitsrelevantes Ereignis das Schulgebäude, die Räumlichkeiten oder Aktenschränke betreffen, aber auch die IT-Systeme.

Das Schulgebäude, die Räumlichkeiten oder Aktenschränke könnten beispielsweise nicht oder unzureichend abgeschlossen sein, so dass unbefugte Personen Zugriff auf die Dokumente mit erhöhtem Schutzbedarf erhalten könnten. Bei den IT-Systemen könnten fehlende/ nicht aktualisierte Virenschutzprogramme oder deaktivierte Firewalls ermöglichen, dass zielgerichtete Cyber-Angriffe die Schule treffen und somit Dokumente der Schülerinnen und Schüler gestohlen oder manipuliert werden könnten.

Die Schulleitung sollte neben einer Dienstanweisung die Lehrkräfte, das Sekretariatspersonal und das weitere Schulpersonal sensibilisieren, damit mögliche Sicherheitsvorfälle schnell erkannt und gemeldet werden können.

Um eine schnelle Reaktion bei der Identifizierung solcher sicherheitsrelevanten Ereignisse zu gewährleisten sollte die Schulleitung den Lehrkräften, dem Sekretariatspersonal und dem weiteren Schulpersonal einen Ansprechpartner für sicherheitsrelevante Fragestellungen bekannt geben, sowie über die Meldewege informieren.

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1	Ansprechpartner – Gebäude, Räume, Schränke	Es wurde ein Ansprechpartner (z.B. Hausmeister) innerhalb der Schule für Sicherheitsfragen bzgl. Gebäude, Räume, Schränke festgelegt.	☐ Ja ☐ Nein
2	Ansprechpartner – IT-Systeme	Es wurde ein Ansprechpartner (z.B. IT-Verantwortlicher) innerhalb der Schule für Sicherheitsfragen bzgl. IT-Systeme festgelegt.	☐ Ja ☐ Nein
3	Ansprechpartner	Allen Lehrkräften, dem Sekretariatspersonal und dem weiteren Schulpersonal sind die Ansprechpartner zu Sicherheitsfragen bei den Gebäuden, Räumen, Schränken und IT-Systemen bekannt. Option 1: Bekanntgabe der Ansprechpartner für Sicherheitsfragen mit Namen, Telefonnummer und E-Mail-Adresse wird im schuleigenen Intranet vorgenommen. Option 2 Bekanntgabe der Ansprechpartner für Sicherheitsfragen mit Namen, Telefonnummer und E-Mail-Adresse wird über ein verteiltes Rundschreiben vorgenommen. Option 3: Bekanntgabe der Ansprechpartner für Sicherheitsfragen mit Namen, Telefonnummer und E-Mail-Adresse wird über einen Aushang im Lehrkräftezimmer oder Sekretariat vorgenommen. Option 4: Schulspezifische Bekanntgabe der Ansprechpartner für Sicherheitsfragen mit Namen, Telefonnummer und E-Mail-Adresse	☐ Ja ☐ Nein ☐ Ja ☐ Nein ☐ Ja ☐ Nein ☐ Ja ☐ Nein ☐ Ja ☐ Nein
4	Protokollierung	Sicherheitsrelevante Ereignisse werden vom Ansprechpartner für Sicherheitsfragen protokolliert.	☐ Ja ☐ Nein
5	Sensibilisierung	Die Lehrkräfte, das Sekretariatspersonal und das weitere Schulpersonal werden durch eine Dienstanweisung der Schulleitung für Sicherheitsvorfälle sensibilisiert.	☐ Ja ☐ Nein

Tabelle 11: Maßnahmen zur Identifizierung und Behandlung sicherheitsrelevanter Maßnahmen

4. Mitarbeiter und Prozesse

4.1 Sensibilisierung und Schulung

4.1.1 Sensibilisierung

Eine dauerhafte Umsetzung und Einhaltung der Maßnahmen zur Informationssicherheit ist nur möglich, wenn ein Verständnis und die Motivation der Lehrkräfte, des Sekretariatspersonals und des weiteren Schulpersonals besonders hoch sind. Um das Sicherheitsbewusstsein aller schulinternen Mitarbeiter/-innen zu fördern und den Stellenwert der Informationssicherheit an der [Name der Schule] zu betonen, sollte von der Schulleitung ein umfassendes, schulweites Sensibilisierungsprogramm erstellt werden, das zum Ziel hat, die Informationssicherheit zu einem integrierten Bestandteil der täglichen Arbeit zu machen.

Das Sensibilisierungsprogramm sollte sowohl organisatorische als auch IT-spezifische Aspekte und Maßnahmen beinhalten. Für das Sensibilisierungsprogramm sollte von der Schulleitung eine verantwortliche Person ernannt werden, die entsprechende Kompetenzen und Qualifikationen im Bereich Informationssicherheit mitbringen. Ziel des Sensibilisierungsprogramms zur Informationssicherheit ist es, die Wahrnehmung aller schulinternen Mitarbeiter/-innen für sicherheitskritische Situationen in den Schulverwaltungsprozessen zu schärfen sowie ihnen die notwendigen Kenntnisse und Kompetenzen für sicherheitsbewusstes Verhalten zu vermitteln.

Das Sensibilisierungsprogramm der [Name der Schule] sollte folgende Punkte umfassen:

Information der Lehrkräfte, des Sekretariatspersonals und des weiteren Schulpersonals über,

- die Informationssicherheitspolitik der Schule. Insbesondere der Schutz von Informationen einer besonders schützenswerten Personengruppe (Kinder und Jugendliche unter 14 Jahren).
- die Informationssicherheitsziele der Schule. Gemeint sind hier die Integrität, Vertraulichkeit und Verfügbarkeit von Informationen (siehe Punkt 1).
    - Gefahren zur Bedrohung der Integrität: technische Fehler, unbefugte Manipulationsversuche (z.B. Computerviren, Schadprogramme), Sabotage, Fahrlässigkeit etc.
    - Gefahren zur Bedrohung der Vertraulichkeit: Spionageaktivitäten, Datenmissbrauch, aber ebenso menschliche Fehler und fehlende Sorgsamkeit etc.
    - Gefahren zur Bedrohung der Verfügbarkeit: kleinere und größere Systemausfälle, Brände, Wasserschäden oder Katastrophen.
- die Organisation und Verantwortlichkeiten im Bereich der Informationssicherheit (siehe folgende Tabelle Punkt 1).
- die ausgewählten Sicherheitsmaßnahmen. Sensibilisierung zu den Maßnahmen, die zur Einhaltung eines gewissen Informationssicherheitsstandards an der Schule

umgesetzt werden (z.B. Zugangskontrollen, Einsatz von Antivieren-Programmen, Backups durchführen etc.).

- die Notwendigkeit, Sicherheitsverstöße zu melden und zu untersuchen (siehe Kapitel 3.6).

Das Sensibilisierungsprogramm der [Name der Schule] kann durch die folgenden unterschiedlichen Maßnahmen dem internen Schulpersonal vermittelt werden:

- regelmäßige Veranstaltungen zum Thema Informationssicherheit bspw. in Form von Informationssicherheits-Workshops oder Fachvorträgen zum Thema insbesondere für das Schulwesen;
- die Schulleitung oder die verantwortlichen Schulmitarbeiter/-innen könnten Publikationen zum Thema in der Schule verbreiten z.B. Infoblätter, Aushänge, Rundschreiben, E-Mail-Newsletter, Presseartikel etc.;
- schriftliche Festlegung der Berichtswege und Handlungsanweisungen im Falle eines vermuteten Sicherheitsproblems (z. B. Auftreten eines Virus, Angriff von außen „Hackern“, …) durch die Schulleitung oder die verantwortlichen Schulmitarbeiter/-innen;
- Formulierung einer Dienstanweisung zur Beachtung der Informationssicherheit in der [Name der Schule] mit dazugehöriger Unterschrift der Kenntnisnahme durch das schulinterne Personal.

Die Maßnahmen zur Umsetzung des Sensibilisierungsprogramms zur Informationssicherheit sollten in regelmäßigen Abständen wiederholt werden, um das vorhandene Wissen aufzufrischen und neue Schulmitarbeiter/ -innen zu informieren. Darüber hinaus sollten alle neuen, beförderten oder versetzten Schulmitarbeiter/ -innen so weit in Fragen der Informationssicherheit geschult werden, wie es der neue Arbeitsplatz verlangt.

Das Sensibilisierungsprogramm ist von der Schulleitung oder die verantwortlichen Schulmitarbeiter/-innen regelmäßig auf seine Wirksamkeit und Aktualität zu überprüfen und laufend an Veränderungen in der Informationssicherheitspolitik der [Name der Schule] sowie an neue Technologien anzupassen.

4.1.2 Schulung

Zusätzlich zum allgemeinen Sensibilisierungsprogramm sind spezielle Schulungen zu den einzelnen Teilbereichen der in diesem Sicherheitskonzept thematisierten Aspekte vorzunehmen, wenn sich dadurch grundlegende Veränderungen beispielsweise im Arbeitsablauf der [Name der Schule] ergeben.

Schulpersonal das in einem besonderen Maß mit Informationssicherheit an der [Name der Schule] zu tun haben (z.B. die Schulleitung, der Informationssicherheitsbeauftragte, Sekretariatspersonal, Lehrkräfte etc.), sind speziell dafür zu schulen. Dazu zählen in der [Name der Schule]

- die Schulleitung;
- die/der (ernannte) Informationssicherheitsbeauftragte ggf. die/der IT-Sicherheitsbeauftragte;
- Sekretariatspersonal/Lehrkräfte die zu internen und vertraulichen Informationen Zugang besitzen (siehe Kapitel 2.1).

Das Schulungsprogramm der [Name der Schule] ist individuell für ihren eigenen individuellen Bedarf durch die Schulleitung oder den Informationssicherheitsbeauftragten zu entwickeln. Zusätzlich kann zur Entwicklung des Schulungsprogramms auch die Unterstützung der oberen und unteren Schulaufsichtsbehörden angefordert werden.

Schulungs- und Sensibilisierungsveranstaltungen zum Thema Informationssicherheit müssen von der Schulleitung oder dem Informationssicherheitsbeauftragten zeitgerecht geplant und umgesetzt werden, um keine Sicherheitslücken durch mangelndes Wissen oder Sicherheitsbewusstsein des Sekretariatspersonals, der Lehrkräfte oder dem sonstigen Schulpersonal entstehen zu lassen.

4.2 Einarbeitung von Sekretariatspersonal, Lehrkräften und sonstigen Schulpersonal

Die Schulleitung, die Lehrkräfte, das Sekretariatspersonal und das sonstige Schulpersonal müssen gewährleisten das neue Schulmitarbeiter/-innen zu Beginn ihrer Beschäftigung an der [Name der Schule] in ihre neuen Aufgaben eingearbeitet und über bestehende Regelungen, Gepflogenheiten und Verfahrensweisen der Schule informiert werden. Die Erstellung einer Checkliste zur Einarbeitung könnte unterstützend wirken.

In der Einarbeitungsphase neuer Schulmitarbeiter/-innen ist insbesondere auf die bestehenden Regelungen und Handlungsanweisungen zur Informationspolitik an der [Name der Schule] hinzuweisen. Sämtliche Schulmitarbeiter/-innen der [Name der Schule] sind über die Regelungen zur Informationssicherheit und deren Veränderungen ständig zu unterrichten, um den Einfluss auf die Schulprozesse bewerten zu können. Ohne eine entsprechende Einweisung kennen die neuen Schulmitarbeiter/-innen die entsprechenden Ansprechpartner/-Innen bzgl. Informationssicherheit (bzw. IT-Sicherheit) nicht. Darüber hinaus wissen die neuen Schulmitarbeiter/-innen nicht, welche IT-Sicherheitsmaßnahmen durchzuführen sind und welche IT-Sicherheitspolitik in der [Name der Schule] betrieben wird. Daraus können Störungen und Schäden für den IT-Einsatz in der [Name der Schule]

entstehen. Aus diesem Grund kommt der geregelten Einarbeitung neuer Mitarbeiter/-innen eine entsprechend hohe Bedeutung zu.

Folgende Maßnahmen sollten bei der Einarbeitung neuer Schulmitarbeiter/-innen berücksichtigt werden:

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1.	Schulung IT-Systeme	Neue Schulmitarbeiter/-innen werden in die Nutzung der für die Stelle wesentlichen IT-Systeme, wie Schulverwaltungssoftware, eingewiesen/ geschult.	☐ Ja ☐ Nein
2.	Sicherheitsmaßnahmen	Mitarbeiterinnen und Mitarbeiter werden zu allen relevanten Sicherheitsmaßnahmen unterrichtet.	☐ Ja ☐ Nein
3.	Ansprechpartner	Alle Ansprechpartner – insbesondere die für Fragen rund um die Informationssicherheit und den Datenschutz – werden vorgestellt.	☐ Ja ☐ Nein
4.	Sicherheitsziele der [Name der Schule]	Die Sicherheitsziele der [Name der Schule] werden verständlich an die neuen Schulmitarbeiter/-innen vermittelt.	☐ Ja ☐ Nein
5.	Potenzielle Risiken der [Name der Schule]	Die potenziellen Risiken der [Name der Schule] werden den neuen Schulmitarbeiter/-innen erläutert.	☐ Ja ☐ Nein
6.	Meldewege bei Sicherheitsvorfällen	Die neuen Schulmitarbeiter/-innen werden über die Verhaltensregeln und Meldewege bei Sicherheitsvorfällen unterrichtet.	☐ Ja ☐ Nein
7.	Schlüssel, Zugangskarten	Die neuen Schulmitarbeiter/-innen erhalten alle notwendigen Schlüssel und Zugangskarten die sie zur Erfüllung ihrer Aufgabe für die [Name der Schule] benötigen.	☐ Ja ☐ Nein

Tabelle 12: Maßnahmen zur Einarbeitung neuer Schulmitarbeiter/-innen:

4.3 Mitarbeiteraustritt

Bei Austritt von Schulpersonal aus der [Name der Schule] ist eine rechtzeitige Einweisung des Nachfolgers durchzuführen, idealerweise durch das ausscheidende Schulpersonal. Ist eine direkte Übergabe nicht möglich, dann ist eine umfassende Dokumentation der Tätigkeiten durch den ausscheidenden Mitarbeiter anzufertigen.

Zusätzlich muss bei einem Ausscheiden von Schulpersonal der [Name der Schule] sichergestellt werden, dass alle im Rahmen ihrer Tätigkeit erhaltenen Unterlagen, Schlüssel und Geräte sowie Ausweise und Zutrittsberechtigungen eingezogen werden. Die Schulleitung oder der ernannte Verantwortliche für die Informationssicherheit ist dafür verantwortlich ein Protokoll der eingezogenen Gegenstände und Dokumente zu erstellen. Alle Daten der Schule oder der Schülerinnen und Schüler sind auf privaten Geräten der ausscheidenden Schulmitarbeiterin/ des Schulmitarbeiters zu löschen.

Der Austritt oder der Aufgabenwechsel einer Schulmitarbeiterin/ des Schulmitarbeiters der [Name der Schule] muss der Schulleitung oder dem ernannten Verantwortlichen der Informationssicherheit rechtzeitig mitgeteilt werden, damit diese bei der IT-Administration beantragen können, dass den ehemaligen Schulmitarbeiterinnen oder Schulmitarbeiter sämtliche Zugriffsberechtigungen auf IT-Systeme entzogen werden bzw. diese bei Aufgabenwechseln angepasst werden.

Vor der Verabschiedung des ausscheidenden Schulpersonals der [Name der Schule] ist explizit darauf hinzuweisen, dass alle Verschwiegenheitserklärungen weiterhin in Kraft bleiben und keine im Rahmen der Tätigkeit erhaltenen Informationen weitergegeben werden dürfen. Das gilt insbesondere für höchst sensible Daten der Schüler, die einen hohen Schutzbedarf besitzen.

Um den Mitarbeiteraustritt geregelt koordinieren zu können ist eine Erstellung einer Checkliste hilfreich, auf denen die einzelnen Aktivitäten des ausscheidenden Personals aufgeführt sind, die sie vor Austritt aus der [Name der Schule] zu erledigen haben.

Folgende Maßnahmen sollten bei Austritt von Schulpersonal aus der [Name der Schule] berücksichtigt werden:

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1.	Einweisung	Der oder die Nachfolger/-in des/r ausscheidenden Mitarbeiters / der Mitarbeiterin wurde umfassend eingewiesen.	☐ Ja ☐ Nein
2.	Rückgabe	Alle Unterlagen, sämtliche Schlüssel sowie Geräte (Speichermedien, mobile Rechner, Dokumentationen etc.) werden zurückgegeben. Alle Daten der Schule und der Schüler auf privaten Geräten werden gelöscht.	☐ Ja ☐ Nein
3.	Verschwiegenheit	Das ausscheidende Schulpersonal wurde explizit darauf hingewiesen, dass sämtliche Verschwiegenheitserklärungen auch nach dem Ausscheiden in Kraft bleiben und dass keine im Arbeitsverhältnis erhaltenen Informationen weitergegeben werden dürfen.	☐ Ja ☐ Nein
4.	Notfallplan	Gehört das ausscheidende Schulpersonal zu den Funktionsträgern in einem Notfallplan? Wenn ja, ist dieser Notfallplan zu aktualisieren und ein Ersatz für die Funktion zu ernennen.	☐ Ja ☐ Nein
5.	Information	Alle Personen, die mit Sicherheitsaufgaben betreut sind (z.B. Pförtner), sind über den Weggang zu informieren.	☐ Ja ☐ Nein
6.	Zutritt	Allen Personen des Schulpersonals ist bewusst, dass der unkontrollierte Zutritt des ausgeschiedenen Mitarbeiters/-in auf das Schulgelände der [Name der Schule], insbesondere aber in Räumlichkeiten der IT-Sicherheit, zu verwehren ist.	☐ Ja ☐ Nein
7.	Zugriff auf Daten	Es ist geklärt auf welche Daten des ausscheidenden Mitarbeiters/der ausscheidenden Mitarbeiterin nach Austritt zugegriffen werden muss.	☐ Ja ☐ Nein
8.	Zugriff auf Arbeitsrechner	Soweit erforderlich: Eine schriftliche Bestätigung für den Zugriff auf den Arbeitsrechner des ausscheidenden Mitarbeiters / der ausscheidenden Mitarbeiterin ist eingeholt.	☐ Ja ☐ Nein

Tabelle 13: Maßnahmen bei Austritt von Schulpersonal

4.4 Vertretungsregelungen

Vertretungsregelungen haben den Sinn, für vorhersehbare (Urlaub, Dienstreise) und auch unvorhersehbare Fälle (Krankheit, Unfall, Kündigung) des Personalausfalls an der [Name der Schule] die Fortführung der Aufgabenwahrnehmung, insbesondere der Informationssicherheitspflicht, zu ermöglichen.

Aus diesem Grund muss vor Eintritt von vorhersehbaren und unvorhersehbaren Personalausfalls geregelt sein, wer wen in welchen Angelegenheiten mit welchen Kompetenzen vertritt. Das ist insbesondere im Bereich der Informationsverarbeitung (Eingabe von Daten in die Schulverwaltungssoftware, Archivierung von Daten etc.) von Bedeutung, da hierfür meist Spezialwissen sowie eine zeitgerechte Einarbeitung von unkundigen Schulpersonal unbedingt erforderlich ist.

Für die [Name der Schule] werden folgende Vertretungsregelungen festgelegt:

Verantwortlich für	**Name, Vorname** **(Berufs-bezeichnung)**	**Vertretung Name, Vorname (Berufs-bezeichnung)**	**Vertretung, Telefon**	**Vertretung, E-Mail**
Informations-sicherheit				
Datenschutz				
Schlüsselverwaltung				
Zugangskontrolle				
Verwaltung IT-Ausstattung/ technische Geräte				
Benutzerrechte IT-Systeme				
Notfallverwaltung				
Gebäudesicherung				
Schulspezifische Verantwortlichkeiten:				

Tabelle 14: Vertretungsregelungen des Schulpersonals

Vertretungsregelungen können effektiv eingesetzt werden, wenn die folgenden Rahmenbedingungen eingehalten werden:

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1.	Projektstand	Zur Übernahme von Aufgaben im Vertretungsfall ist der Verfahrens- oder Projektstand hinreichend dokumentiert.	☐ Ja ☐ Nein
2.	Schulung	Die Vertreter/-innen werden so geschult, dass sie die Aufgaben jederzeit übernehmen können.	☐ Ja ☐ Nein
3.	Aufgabenumfang	Es ist festgelegt, welcher Aufgabenumfang im Vertretungsfall von wem wahrgenommen wird.	☐ Ja ☐ Nein
4.	Zugangs-Zutrittsberechtigungen	Die Vertreter/-innen erhalten die erforderlichen Zugangs- und Zutrittsberechtigungen nur im Vertretungsfall von der Schulleitung der [Name der Schule] oder dem Verantwortlichen für die Informationssicherheit.	☐ Ja ☐ Nein
5.	Information	Alle Personen, die mit Sicherheitsaufgaben betreut sind (z.B. der Pförtner) werden über den Vertretungsfall informiert.	☐ Ja ☐ Nein
6.	Externe Mitarbeiter	Ist es in Ausnahmefällen nicht möglich, für Personen kompetente Vertreter/-innen zu benennen oder zu schulen, werden frühzeitig externe Mitarbeiter/-innen (z.B. aus der unteren/oberen Schulaufsichtsbehörde) für den Vertretungsfall eingesetzt oder rekrutiert.	☐ Ja ☐ Nein

Tabelle 15: Rahmenbedingungen der Vertretungsregelungen

4.5 Fremdpersonal

Bei der Beschäftigung von Fremdpersonal muss grundsätzlich, wie bei allen internen Mitarbeitern der [Name der Schule], auf die Einhaltung aller geltenden Gesetze, Vorschriften und internen Regelungen (insbesondere die Informationssicherheit) verpflichtet werden.

Fremdpersonal das nur kurzfristig oder einmalig in der [Name der Schule] zum Einsatz kommt (z.B. Besucher/-innen, Handwerker/-innen, Wartungs- und Reinigungspersonal etc.) kann wie Besucher behandelt werden und muss in sicherheitsrelevanten Bereichen der [Name der Schule] beaufsichtigt werden. Bei längerfristig beschäftigten Fremdpersonal wiederum muss das Fremdpersonal in ihre Aufgaben eingewiesen werden. Für langfristig beschäftigtes Fremdpersonal gilt ebenso die Vertretungsregel wie für das interne Schulpersonal der [Name der Schule].

Bevor externes Schulpersonal Zugang und Zugriff zu vertraulichen Informationen erhalten, müssen mit Ihnen Vertraulichkeitsvereinbarungen abgeschlossen werden. Hierfür können standardisierte Vorlagen/ Muster zu Vertraulichkeitsvereinbarungen für externes Schulpersonal speziell für Schulen aus Schleswig-Holstein vom Unabhängigen Landeszentrum für Datenschutz (ULD) verwendet werden.[2]

Bei einem Austritt des Fremdpersonals aus der [Name der Schule] muss, analog zu schulinternem Personal, eine Übergabe- und Rückgabe der Arbeitsergebnisse und ausgehändigter Zutritts- bzw. Zugangsberechtigungen erfolgen.

[2] Siehe https://www.datenschutzzentrum.de/uploads/schulen/dokumente/verschwiegenheitsverpflichtung-externe-mitarbeiter.pdf), letzte Aktualisierung: 12.06.2019, 17:25

Folgende Anforderungen sollten bei der Beschäftigung von Fremdpersonal berücksichtigt werden:

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1.	Schulung IT-Systeme	Das Fremdpersonal wird in die Nutzung der für die Stelle wesentlichen IT-Systeme, z.B. Schulverwaltungssoftware, eingewiesen/ geschult.	☐ Ja ☐ Nein
2.	Sicherheitsmaßnahmen	Das externe Personal wird zu allen relevanten Sicherheitsmaßnahmen unterrichtet.	☐ Ja ☐ Nein
3.	Ausreichend Zeit	Dem Fremdpersonal wird ausreichend Zeit zum Einarbeiten gegeben ggf. löschen von Daten.	☐ Ja ☐ Nein
4.	Ansprechpartner	Alle Ansprechpartner – insbesondere die für Fragen rund um die Informationssicherheit und den Datenschutz – werden vorgestellt.	☐ Ja ☐ Nein
5.	Sicherheitsziele der [Name der Schule]	Die Sicherheitsziele der [Name der Schule] werden verständlich an das Fremdpersonal vermittelt.	☐ Ja ☐ Nein
6.	Potenzielle Risiken der [Name der Schule]	Die potenziellen Risiken der [Name der Schule] werden dem Fremdpersonal erläutert.	☐ Ja ☐ Nein
7.	Meldewege bei Sicherheitsvorfällen	Das neue Fremdpersonal wird über die Verhaltensregeln und Meldewege bei Sicherheitsvorfällen unterrichtet.	☐ Ja ☐ Nein
8	Schlüssel, Zugangskarten	Das Fremdpersonal erhält alle notwendigen Schlüssel und Zugangskarten die es zur Erfüllung der Aufgabe für die [Name der Schule] benötigt.	☐ Ja ☐ Nein
9	Verschwiegenheits-verpflichtung	(Längerfristiges) Fremdpersonal hat die Verschwiegenheitsverpflichtung gem. ULD zu unterschreiben und bei der [Name der Schule] einzureichen.	☐ Ja ☐ Nein

Tabelle 16: Anforderungen zur Beschäftigung von Fremdpersonal

4.6 Vergabe und Verwaltung von Berechtigungen

Die Schulleitung oder der Verantwortliche für die Informationssicherheit der [Name der Schule] muss festlegen, welche Zutritts-, Zugangs- und Zugriffsrechte an welches Schulpersonal im Rahmen ihrer Aufgaben und Funktionen vergeben werden sollen. Dabei ist zu beachten, dass nur so viele Rechte vergeben werden, wie für die Aufgabenwahrnehmung notwendig ist. Um das zu erreichen, muss ein geregelter Prozess für die Vergabe (sog. Identitäts- und Berechtigungsmanagement), die Verwaltung und den Entzug von Berechtigungen etabliert werden der darüber hinaus aktuell und vollständig dokumentiert werden muss.

Unter Identitätsmanagement versteht man allgemein, dass Benutzer, die auf die Ressourcen einer Institution zugreifen zweifelsfrei identifiziert und authentifiziert werden. Die Verwaltung der dafür notwendigen Informationen wird als Identitätsmanagement bezeichnet. Das Berechtigungsmanagement hingegen legt fest, ob und wie Benutzer auf Informationen oder Dienste zugreifen und diese benutzen dürfen. Den Benutzern ist dementsprechend, basierend auf ihrem Benutzerprofil, Zutritt, Zugang oder Zugriff zu gewähren oder zu verweigern. Berechtigungsmanagement bezeichnet somit die Prozesse, die für die Zuweisung, Entzug und Kontrolle der Rechte erforderlich sind.

Folgende Anforderungen müssen zur Etablierung eines funktionierenden Identitäts- und Berechtigungsmanagements in der [Name der Schule] erfüllt werden:

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1.	Verantwortlicher	Die Schulleitung oder der/die Verantwortliche für Informationssicherheit der [Name der Schule] hat einen Verantwortlichen ernannt, der für die Vergabe und Verwaltung von Berechtigungen zuständig ist.	☐ Ja ☐ Nein
2.	Benutzergruppen	Der/die Verantwortliche für die Berechtigungen der [Name der Schule] hat Benutzergruppen (z.B. Schulleitung, Sekretariatspersonal, Lehrkräfte etc.) festgelegt, die alle über separate Rollen verfügen.	☐ Ja ☐ Nein
3.	Tatsächlicher Bedarf	Der/die Verantwortliche für die Berechtigungen der [Name der Schule] hat sichergestellt, dass Benutzerkennungen und Berechtigungen nur aufgrund des tatsächlichen Bedarfs vergeben werden. Bei personellen Veränderungen müssen, die nicht mehr benötigten Benutzerkennungen und Berechtigungen entfernt werden. Wenn das Schulpersonal zusätzliche Berechtigungen beantragen, dann dürfen diese nur nach Begründung durch den Verantwortlichen für Berechtigungen vergeben werden.	☐ Ja ☐ Nein

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
4.	Dokumentation	Der/die Verantwortliche für die Berechtigungen der [Name der Schule] dokumentiert sämtliche Benutzer, angelegte Benutzergruppen und Rechteprofile des Schulpersonals. Diese Dokumentation wird regelmäßig auf Aktualität überprüft und vor unberechtigtem Zugriff geschützt.	☐ Ja ☐ Nein
5.	Zutritts-, Zugangs- und Zugriffsberechtigungen	Der/die Verantwortliche für die Berechtigungen der [Name der Schule] hat festgelegt, welche Zutritts-, Zugangs- und Zugriffsberechtigungen an welche Personen der Schule im Rahmen ihrer Funktion vergeben werden. Wenn Zutrittsmittel wie Schlüssel, Chipkarten etc. verwendet werden, müssen diese bei Ausgabe bzw. Entzug dokumentiert werden.	☐ Ja ☐ Nein
6.	Bildschirmsperre	Die in der der [Name der Schule] eingesetzten Softwareprodukte verfügen über eine Bildschirmsperre die bei längerer Pausenzeit der Benutzer/-innen automatisch aktiv werden und die aktuell auf dem Bildschirm vorhandenen Informationen verbergen.	☐ Ja ☐ Nein

Tabelle 17: Maßnahmen des Identitäts- und Berechtigungsmanagements

5. IT-Sicherheit

5.1 Hardware

Die Bestandteile eines Computers werden in die beiden Bereiche Hardware und Software unterteilt. Als Hardware bezeichnet man alle physisch vorhandenen Komponenten die als Grundausstattung eines PCs bzw. Notebooks immer aus denselben Komponenten besteht.

Räume in denen Hardware-Komponenten aufgebaut werden (z.B. mit Netzstrukturen und IT-Systemen), die den Zugang auf das Verwaltungsnetz der Schulen bzw. auf das kommunale Schulträgernetz bereitstellen, unterliegen besonderen Schutzmaßnahmen. Insbesondere, da die entsprechenden Gebäude der Öffentlichkeit während und ggf. außerhalb der regulären Dienstzeiten (z.B. Schulfeste oder Schule als Wahllokal) zugänglich sind. Es müssen somit Maßnahmen und Regelungen getroffen werden, um den unberechtigten Zutritt zu schutzbedürftigen Räumen zu verhindern. (Siehe auch Kapitel 3.2).

Die Hardware ist nicht nur vor unbefugten Zugriffen zu schützen, sondern auch vor Beschädigung durch Feuer, Wasser oder Diebstahl. Daher sind Hauptrechner oder Server in einem separaten, geschützten Raum aufzustellen. Darüber hinaus muss die zentrale Netzwerktechnik wie Router, Switches und Hubs in gesicherten, nicht öffentlich zugänglichen Räumen oder Schutzschränken untergebracht werden.

5.1.1 Verwaltungsrechner

Die Auswahl der eingesetzten Schulverwaltungsrechner hängt maßgeblich davon ab, ob sie stationär oder mobil eingesetzt werden soll.

Stationäre Geräte können in Lehrerzimmern, Lehrerarbeitsräumen und Büros aufgestellt werden. Mobile Geräte sind entweder in größerer Menge in Laptopwagen oder in kleinerer Anzahl in Koffersystemen transportabel einsetzbar.

Der Einsatz von Schulverwaltungsrechnern für die Schulleitung, das Sekretariatspersonal und der Lehrkräfte wird i.d.R. stationär in den Räumlichkeiten des entsprechenden Schulpersonals betrieben. Hinsichtlich der Hard- und Softwarevoraussetzungen sind die Vorgaben für Landesnetzrechner zu beachten. Genauere Informationen können hier beim IQSH eingeholt werden.[3]

Unabhängig davon, wer den Schulverwaltungsrechner zur Verfügung stellt oder wer das Schulverwaltungssystem administriert, ist die Schulleitung bzw. der ernannte Verantwortliche der Informationssicherheit der [Name der Schule] dafür verantwortlich, die folgenden Anforderungen zu beachten.

Auch wenn die Hardware und die Software vom Schulträger bezahlt werden, hat dieser hinsichtlich des Umganges mit der EDV keine freie Entscheidungskompetenz. Die Schule als Daten verarbeitende Stelle wird von Ihnen verantwortlich vertreten. Damit ist nur die Schulleitung bzw. der ernannte Verantwortliche der Informationssicherheit der [Name der Schule] entscheidungsbefugt. Das bedeutet, dass Änderungen am EDV-System vorher von der Schulleitung bzw. dem ernannten Verantwortlichen der Informationssicherheit der [Name

[3] Siehe IT Ausstattungsempfehlung 2015 des IQSH, Kapitel 5, veröffentlicht im August 2015.

der Schule] genehmigt werden müssen. Sämtliche Änderungen des EDV-Systems sind lückenlos zu dokumentieren.

Zur genauen Konfiguration eines Schulverwaltungsrechners sind die Dienstanweisung für die Nutzung der Schulverwaltungsrechner im Landesnetz Bildung (LanBSH)[4], die Angaben des Praxishandbuchs Schuldatenschutz[5] (aktuell S. 117) sowie die jährlichen Empfehlungen für die schulische IT- und Medienausstattung in Schleswig-Holstein des IQSH zu berücksichtigen[6].

Folgende Anforderungen sollten zum Aufbau eines Schulverwaltungsrechners im Landesnetz Bildung berücksichtigt werden:

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1	Verarbeitung personenbezogener Daten	Die Verarbeitung personenbezogener Daten von Schülerinnen und Schülern, Eltern und Lehrkräften sowie von vertraulichen verwaltungsbezogenen Informationen wird nur auf den speziell konfigurierten Schulverwaltungsrechnern durchgeführt.	☐ Ja ☐ Nein
2	Kein direkter Internetanschluss	Die Schulverwaltungsrechner sind nicht direkt an das Internet angeschlossen. Sie sind ausschließlich über das gesicherte LanBSH angebunden.	☐ Ja ☐ Nein
3	Dienstliche Zwecke	Die Schulverwaltungsrechner werden nur für dienstliche Zwecke von den dazu berechtigten Nutzerinnen und Nutzern verwendet. Hierbei handelt es sich grundsätzlich um die im § 6 SchulDSVO genannten Personenkreise.	☐ Ja ☐ Nein
4	Verwaltung der Benutzer	Sämtliche Benutzerinnen und Benutzer des Landesnetzes Bildung sind im Verzeichnisdienst des Landes verwaltet. (Die Administration erfolgt im Regelfall durch das IQSH oder durch den Schulträger, die die Benutzerverwaltung ihrer Schulen verantwortlich übernommen haben.)	☐ Ja ☐ Nein
5	Benutzername und Kennwort	Jede im Verzeichnisdienst als berechtigt registrierte Person meldet sich mit ihrem individuellen Benutzernamen und dem zugehörigen Kennwort für die Nutzung des Schulverwaltungsrechners an.	☐ Ja ☐ Nein

[4] Siehe Dienstanweisung für die Nutzung der Schulverwaltungsrechner im Landesnetz Bildung (LanBSH) des MBWK, veröffentlicht am 03.07.2017.

[5] Siehe Praxishandbuch Schuldatenschutz des ULD Schleswig-Holstein, S.117, veröffentlicht im Jahre 2009.
[6] Siehe IT Ausstattungsempfehlung 2015 des IQSH, S.12, veröffentlicht im August 2015.

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
6	Kennwortrichtlinien	Das Startkennwort für die erste Anmeldung ist vorgegeben. Jede Benutzerin und jeder Benutzer erstellt danach ein neues Kennwort für sich selbst. Es muss mindestens aus acht Zeichen bestehen. Aufgrund der Kennwortrichtlinie[7] müssen darin jeweils mindestens ein Buchstabe, eine Zahl und mindestens ein Sonderzeichen enthalten sein.	☐ Ja ☐ Nein
7	Sperrbildschirm	Auf jedem Schulverwaltungsrechner ist ein Sperrbildschirm mit Kennwortschutz eingerichtet. Er wird nach 10 Minuten ohne Aktivität am Computer automatisch eingeschaltet. Diese Einstellung ist vorgegeben und nicht veränderbar. Bei Verlassen des Arbeitsplatzes − auch bei kurzfristiger Abwesenheit − ist der Computer eigenständig zu sperren, d. h. der Sperrbildschirm ist zu aktivieren (z. B. durch Drücken der Tastenkombination „Windows-Taste + L“).	☐ Ja ☐ Nein ☐ Ja ☐ Nein

Tabelle 18: Anforderungen zum Aufbau eines Schulverwaltungsrechners im LanBSH

[7] Siehe Dienstanweisung für die Nutzung der Schulverwaltungsrechner im Landesnetz Bildung (LanBSH) des MBWK, veröffentlicht am 03.07.2017.

5.1.2 Netzwerke

Die meisten Schulen Schleswig-Holsteins tauschen ihre Informationen und Daten über Rechnernetze aus, die nicht nur herkömmliche Endgeräte miteinander verbinden, sondern auch weitere mobile Endgeräte einbinden. Durch die damit verbundenen verschiedenen Eintrittsmöglichkeiten der Endgeräte und Dienste in das Netzwerk ist es wichtig, das eigene Netz durch eine sichere Netzarchitektur zu schützen. Hierfür muss zum Beispiel geplant werden, wie ein lokales Netzwerk (LAN) oder ein drahtloses Netzwerk (WLAN) sicher aufgebaut werden kann.

Zum Aufbau einer sicheren Netzarchitektur ist es wichtig bei der Einrichtung des schulischen Netzwerkes die perspektivische Entwicklung zu betrachten, da sonst die Gefahr besteht in technologische Sackgassen zu investieren. Wenn es geplant ist, schülereigene Endgeräte im Schulalltag zu integrieren, sollte die Netzwerkstruktur im Allgemeinen und die WLAN-Infrastruktur im Speziellen so ausgelegt sein, dass sie ohne große Umbaumaßnahmen erweiterbar und an den jeweiligen Bedarf anpassbar sind (Skalierbarkeit). Diese Überlegungen sind im Rahmen der Erstellung oder Fortschreibung eines Mediennutzungsplanes der [Name der Schule] einzubeziehen.

Um einen störungsfreien und informationstechnisch einwandfreien Betrieb des schulischen Netzwerks zu gewährleisten, müssen die verschiedenen Bereiche strikt voneinander getrennt sein (vgl. § 11 Abs. 2 und 3 SchulDSVO -> Verwaltungsnetz, päd. Netz). Das kann erreicht werden, indem für jedes Netz eigene Switches in den Netzwerkschränken einbaut werden oder bei einer zunehmenden Anzahl von Netzwerken auf VLANs (Virtual Local Area Network) zurückgriffen wird.

Für die Durchführung verschiedener organisatorischer und administrativer Aufgaben bei der Netzwerkverwaltung werden an vielen Schulen Server eingesetzt. Bei der Auswahl eines Servers ist – neben der Dimensionierung der Hardware – die zentrale Frage welches System auf dem Server installiert werden soll. Dabei werden die beiden häufigsten Optionen entweder ein Gerät mit Windows-Serverbetriebssystem oder ein spezieller Schulserver sein. Im Regelfall sind alle wichtigen Funktionen wie Benutzerverwaltung, Softwareverteilung, Internetfilter usw. in diesen Systemen vereint und an die schulische Nutzung angepasst. Sie sind in der Bedienung – im besten Falle – so aufgebaut, dass auch Lehrkräfte ohne Administrationskenntnisse bspw. Passwörter zurücksetzen können.

5.1.2.1 Internetnutzung

Bei der Nutzung des Internets für schulische Zwecke sind verschiedene organisatorische, technische und rechtliche Aspekte zu beachten[8]. Abhängig von der angedachten Nutzerzahl und den angedachten Anwendungen eines schulischen Netzwerkes ist zunächst die ausreichende Internetversorgung zu berücksichtigen. Gerade bei hohen Nutzerzahlen sind VDSL- und Glasfaseranschlüsse oder alternativ schnelle Richtfunkanbindungen zu bevorzugen. Über geeignete Lösungen ist durch die Schule soweit wie möglich sicherzustellen, dass minderjährige Schüler und Schülerinnen keinen Zugriff auf jugendgefährdende Inhalte bekommen. Eine Internetfilterung unterstützt dabei und sorgt für einen ausreichenden Jugendmedienschutz und die rechtliche Absicherung der Schule. Wenn eine unbeaufsichtigte Nutzung des Internets erfolgt, sind bestenfalls alle Anmeldevorgänge

[8] Siehe Themenpapier Internetnutzung in Schulen vom IQSH

und die anschließenden Nutzeraktivitäten im Internet personenbezogenen zu protokollieren und für einen festgelegten Zeitraum zu speichern. Damit ist sichergestellt, dass die Schule bei strafrechtlichen Verstößen oder zivilrechtlichen Forderungen den Verursacher/ die Verursacherin des Schadens ermitteln kann.

Jede Schule muss für die Internetnutzung der Schüler/-innen eine Nutzungsordnung erstellen, in der die wichtigsten Regeln und Vorgaben für die schulische Internetnutzung festgelegt sind. Sie sollte durch die Schulkonferenz beschlossen werden. Alle Schüler/-innen und ihre Eltern haben eine entsprechende Kenntnisnahme der Nutzungsordnung zu unterzeichnen, bevor der Zugang zum Internet freigeschaltet wird. Die Hinweise zum Jugendmedienschutz und zur benutzerbezogenen Protokollierung gelten bei der Nutzung von WLAN in besonderem Maße, da gerade beim Einsatz mobiler Endgeräte eine permanente Beaufsichtigung nur schwer zu gewährleisten ist. Da zunehmend auch schüler- beziehungsweise lehrereigene Geräte im Netz verwendet werden, sollte zudem eine Beschränkung des Schulnetzes auf bekannte und registrierte Geräte vorgenommen werden, um einem Missbrauch entgegenzuwirken. Detaillierte Informationen hierzu finden sich in dem Themenpapier „Internetnutzung in Schulen“[9].

5.1.2.2 WLAN

Beim Aufbau einer WLAN-Infrastruktur ist eine umfassende Planung von großem Vorteil, damit eine zuverlässige und ausreichend leistungsfähige Funktionalität des Systems gewährleistet werden kann.

Bei der WLAN-Ausstattung größerer Bereiche bzw. ganzer Schulgebäude wird der Einsatz zentral administrierbarer Systeme empfohlen. Das bedeutet, dass alle Access Points zentral über eine Oberfläche verwaltet und miteinander verbunden werden können. Entsprechend leistungsfähige Access Points können auch über verschiedene SSIDs mehrere voneinander getrennte Netze anbieten. Damit können die entsprechend gestalteten VLAN-Strukturen im LAN auch im WLAN abgebildet und so auch dort für getrennte Netze gesorgt werden. Aufgrund der besonderen Anforderungen in Bezug auf den Datenschutz und die Datensicherheit ist derzeit die Nutzung von WLAN für die Schulverwaltung im Landesnetz Bildung nicht zulässig.

Bei der WLAN-Nutzung müssen die Benutzer grundsätzlich dafür sensibilisiert werden, dass der zusätzliche Komfort durch die Mobilität des Netzwerkzugangs damit verbunden ist, dass zusätzliches Gefährdungspotential durch die drahtlose Kommunikation entsteht. Im Hinblick auf die Informationssicherheit ist den Benutzern somit zu verdeutlichen, dass zusätzliche Sicherheitsmaßnahmen notwendig sind, um das Abhören und Auswerten von WLAN-Kommunikation zu verhindern.

Weitere Sicherheitshinweise zur WLAN-Nutzung finden sich im Themenpapier Internetnutzung des IQSH.[10]

[9] Siehe Themenpapier Internetnutzung in Schulen vom IQSH

[10] https://www.schleswig-holstein.de/DE/Landesregierung/IQSH/Arbeitsfelder/ITMedien/Material/Downloads/themenpapierInternetnutzung.pdf

5.1.3 Mobile Endgeräte (dienstlich bereitgestellt)

Unter mobilen IT-Geräten sind alle für einen mobilen Einsatz geeigneten Geräte zu verstehen, wie etwa Smartphones, Tablet-PCs, mobile Datenträger wie USB-Festplatten und -Sticks (siehe auch Kapitel 5.1.4). Sie sind vielfältigeren Risiken ausgesetzt als solche, die sich innerhalb geschützter Räumlichkeiten befinden und stationär eingesetzt werden.

Werden mobile Endgeräte (Smartphones, Notebooks, Tablets) zur Erfüllung der schulischen Aufgaben eingesetzt, müssen die Informationen mit den geeigneten organisatorischen und technischen Maßnahmen geschützt werden und dürfen in keiner Form anders als über das Landesnetz Bildung mit dem Internet verbunden werden.

Die Sicherheitsmaßnahmen für mobile Endgeräte unterscheiden sich nicht wesentlich von den allgemeinen Vorgaben der Dienstanweisung für Schulverwaltungsrechner entsprechend der Checkliste in Kapitel 5.1.1.

Da die Nutzenden die mobilen Endgeräte auch außerhalb der Schule verwenden könnten, sind die mobilen Endgeräte auch außer Haus sicher aufzubewahren. Hierfür können nur einige Hinweise gegeben werden, die bei der mobilen Nutzung zu beachten sind:

- Die Nutzenden mobiler IT-Geräte sind über die potenziellen Gefahren bei Mitnahme und Nutzung eines solchen Gerätes außerhalb der geschützten Umgebung eingehend zu informieren und zu sensibilisieren. Dies sollten in schriftlicher Form - etwa als Merkblatt - erfolgen;
- Werden auf mobilen IT-Geräten eingeschränkte, vertrauliche, geheime oder streng geheime bzw. personenbezogene oder sensible Daten gespeichert und verarbeitet, so ist die Installation eines Zugangs- bzw. Zugriffsschutzes (über Passwort, Dongle, Chipkarte etc.) sowie einer Festplatten- oder Dateiverschlüsselung dringend zu empfehlen;
- Geräte dürfen nicht unbeaufsichtigt liegen gelassen oder aufbewahrt werden.
- Einige Geräte bieten zusätzlich die Möglichkeit zum Anketten des Gerätes (bspw. Kensington Lock). Der Diebstahl setzt dann den Einsatz von Werkzeug voraus.
- Bei jedem Wechsel des Besitzers/der Besitzerin müssen alle benötigten Zugangsmechanismen (z. B. Passwörter) gesichert weitergegeben bzw. erneuert werden.

5.1.4 Einsatz privater informationstechnischer Geräte

Für die Ausübung ihres Dienstes ist es Lehrkräften gem. §14 SchulDSVO erlaubt ihre privaten informationstechnischen Geräte zur Verarbeitung personenbezogener Daten der betroffenen Personen zu verwenden, soweit ihnen hierfür zuvor eine schriftliche Genehmigung der Schulleitung erteilt worden ist. Verantwortlich bleibt auch in diesem Fall die jeweilige Schule. Ein Musterantragsformular zur Genehmigung des Einsatzes von privaten informationstechnischen Geräten wird vom für Bildung zuständigen Ministerium zur Verfügung gestellt.[11] Die von den Lehrkräften abzugebende Zusicherung stellt eine

[11] Siehe Informationsportal: www.Schuldatenschutz.Schleswig-Holstein.de

dienstliche Erklärung dar. Weitere Vorgaben zu den Bestandteilen des Genehmigungsschreibens werden in §14 SchulDSVO gegeben.

Der Gebrauch von privaten informationstechnischen Geräten durch die Lehrkräfte entbindet die für die Datenverarbeitung verantwortliche Schulleitung oder die dafür verantwortliche Person nicht von ihrer Kontrollfunktion bezüglich des Umfanges, der Rechtmäßigkeit und der Ordnungsmäßigkeit der Datenverarbeitung.

Die Formulierung „informationstechnische Geräte“ umfasst nicht nur PC oder Laptop sondern auch Wechseldatenträger wie DVD, USB-Stick usw.. Um einen ausreichenden Schutz der personenbezogenen Daten bei der Verarbeitung im häuslichen Bereich zu gewährleisten, sollten alle personenbezogenen Daten generell verschlüsselt und auf einem externen Datenträger (USB-Stick) gespeichert werden. Darüber hinaus sind die die technischen Maßnahmen aus Kapitel 5.1.3 zu beachten. Für die Verschlüsselung bietet sich beispielsweise das OpenSource-Produkt TrueCrypt an. Das IQSH stellt eine Version dieser Software zum Download bereit, die speziell auf USB-Sticks zugeschnitten ist, und keine Installation des Programms auf dem eigenen Rechner erfordert.[12] Auch eine Verschlüsselung von Dokumenten direkt aus Office-Anwendungen durch ein verschlüsselndes Kennwort ist eine wirksame Maßnahme.

Im Umgang insbesondere mit sensiblen Schuldaten nicht geeignet bzw. nicht zulässig sind für private technische Geräte:

- Kommunikation via WhatsApp oder ähnlichen Messenger-Programmen.
- Ablage von sensiblen Daten in Cloudspeichern (bspw. Dropbox, Google Drive, Apple Drive etc.).
- Versand personenbezogener Daten durch Standard-E-Mail ohne Verschlüsselung.
- Unverschlüsselte Festplatten (Zugangssicherung, Reparaturen). Zu beachten ist, dass auch eine verschlüsselte Festplatte nach dem Hochfahren während des gesamten Betriebs des Computers sichtbar ist.
- Automatische Anmeldung am PC oder Notebook ohne Eingabe eines Passwortes.

Die Schulleitungen sollten im Vorwege durch klare Vorgaben (Dienstanweisung) solche unrechtmäßigen Datenabgänge unterbinden. Insbesondere ist sicherzustellen, dass keine automatischen Weiterleitungen von Schuladressen zu privaten E-Mail-Konten erfolgen, da die Absender im falschen Glauben gelassen würden, ihre E-Mail werde nur über eine sichere Umgebung geleitet. Sobald jedoch eine E-Mail unverschlüsselt über einen privaten Mailserver (z.B. GMX, Gmail etc.) geleitet wird, ist diese in den Zugriff Dritter gelangt, was nicht zulässig ist.

Wenn die Nutzung von privaten E-Mail-Konten von den Schulbetreibern mangels schulextern zugänglichen Geschäftsadressen geduldet wird, muss die Schule angemessene organisatorische und technische Maßnahmen umsetzen, um sensible Daten zu schützen und auch die Lehrpersonen vor Haftungsklagen zu bewahren. E-Mails mit vertraulichem

[12] https://fit.lernnetz.de/doku.php?id=themen:mobiler-datensafe (letzter Zugriff: 13.01.2020 – 10:00Uhr)

Inhalt müssen verschlüsselt sein, da der Datentransfer außerhalb des Landesnetzes nicht ausnahmslos als sicher anzunehmen ist (vgl. § 9 Abs. 5 SchulDSVO).

Weitere Anforderungen zur Benutzung privater technischer Endgeräte sind der Checkliste in Kapitel 5.1.1 zu entnehmen.

5.1.5 Speichermedien

Handelsübliche PCs sind heute in der Regel mit CD-/DVD-ROM-Laufwerk bzw. CD-/DVD-Writer ausgestattet. Zusätzlich besteht die Möglichkeit, über Schnittstellen externe Speichermedien anzuschließen, die von neueren Betriebssystemen automatisch erkannt werden. Beispiele sind USB-Sticks bzw. -Festplatten, die in die USB-Schnittstelle gesteckt werden. Durch solche Laufwerke für Wechselmedien und externe Datenspeicher ergeben sich potenzielle Sicherheitsrisiken:

- Der PC könnte von solchen Laufwerken unkontrolliert gebootet/gestartet werden und damit Sicherheitseinstellungen außer Kraft gesetzt werden;
- Es könnte unkontrolliert Fremdsoftware (auch Schadsoftware, Viren, Trojanische Pferde) von solchen Laufwerken eingespielt werden;
- Dienstliche Daten könnten unberechtigt auf Wechselmedien kopiert werden.

Diesen Gefahren muss durch geeignete organisatorische oder technische Sicherheitsmaßnahmen entgegengewirkt werden. Hierfür bieten sich verschiedene Vorgehensweisen an, deren spezifische Vor- und Nachteile im Folgenden kurz dargestellt werden:

- Ausbau von Laufwerken: Der Ausbau der Laufwerke für Wechselmedien (bzw. der Verzicht bei der Beschaffung) bietet zwar den sichersten Schutz vor den oben genannten Gefährdungen, ist aber meist mit erheblichem Aufwand verbunden. Weiter ist zu berücksichtigen, dass der Ausbau unter Umständen die Administration und Wartung des IT-Systems behindert.
- Deaktivierung im EFI/BIOS bzw. Betriebssystem: Im EFI/BIOS bieten die meisten PCs Einstellmöglichkeiten dafür, von welchen Laufwerken gebootet werden kann. In Verbindung mit einem Passwortschutz der BIOS-Einstellungen (siehe auch BSI M 4.84 Nutzung der BIOS-Sicherheitsmechanismen) kann dadurch das unkontrollierte Booten von Wechselmedien und mobilen Datenträgern unterbunden werden. Des Weiteren können die vorhandenen Laufwerke und Schnittstellen bei modernen Betriebssystemen einzeln deaktiviert werden. Die Deaktivierung der Laufwerke im EFI/BIOS bzw. Betriebssystem hat den Vorteil, dass keine Hardwareänderungen erforderlich sind.
- Kontrolle der Schnittstellennutzung: Der Betrieb von externen Speichermedien wie USB -Sticks lässt sich nur sehr schwer verhindern, wenn die verwendete Schnittstelle auch für andere (erlaubte) Zusatzgeräte genutzt wird. So werden beispielsweise Notebooks ausgeliefert, die zum Anschluss einer Maus nur die USB-Schnittstelle zur Verfügung stellen. Dadurch ist es in der Regel nicht sinnvoll, ein „USB-Schloss“ zu verwenden oder die Schnittstelle durch andere Maßnahmen zu deaktivieren.

- Verschlüsselung: Es gibt Produkte, die dafür sorgen, dass ausschließlich Zugriffe auf dafür zugelassene mobile Datenträger möglich sind. Eine Lösung ist beispielsweise, dass nur noch mobile Datenträger gelesen und beschrieben werden können, die mit bestimmten kryptographischen Schlüsseln verschlüsselt worden sind. Dies schützt nicht nur vor unbefugtem Zugriff über manipulierte mobile Datenträger, sondern schützt auch die Daten auf den mobilen Datenträgern bei Verlust oder Diebstahl.

Bei der Auswahl einer geeigneten Vorgehensweise müssen immer alle Laufwerke für Wechselmedien berücksichtigt werden, aber ebenso alle Möglichkeiten, über Vernetzung Daten auszutauschen, also insbesondere auch E-Mail und Internetanbindungen. Wenn der PC über eine Verbindung zum Internet verfügt, ist es nicht allein ausreichend, alle Laufwerke für Wechselmedien zu deaktivieren oder auszubauen. Besonderes Augenmerk ist auf den Schutz vor Schadprogrammen, z.B. Computerviren oder „Trojanische Pferde“, zu richten.

Damit die Sicherheitsmaßnahmen akzeptiert und beachtet werden, müssen die Nutzenden über die Gefährdung durch Laufwerke für Wechselmedien informiert und sensibilisiert werden.

Die Handhabung von Wechseldatenträgern wurde vom Land Schleswig-Holstein zusätzlich in der Dienstanweisung für die Nutzung der Schulverwaltungsrechner im Landesnetz Bildung (LanBSH) geregelt.[13] Im Folgenden Abschnitt werden die wesentlichen Vorgaben kurz skizziert:

- USB-Datenträger können für erforderliche temporäre Speicherungen dienstlicher Daten (z. B. für die Zeugniserstellung) genutzt werden. Hierfür dürfen ausschließlich dienstlich zur Verfügung gestellte USB-Datenträger verwendet werden.

- Außerhalb der Schulverwaltung dürfen diese nur mit gemäß § 14 SchulDSVO genehmigten privaten informationstechnischen Geräten der Lehrkräfte verwendet werden.

- Sofern auf den USB-Datenträgern personenbezogene oder vertrauliche Daten gespeichert sind, sind diese nach dem Stand der Technik zu verschlüsseln. Die Vergabe des Verschlüsselungspasswortes hat nach den Vorgaben unter Kapitel 3.2. zu erfolgen. Verschlüsselungspasswörter sind in der Schulverwaltung in einem verschlossenen Umschlag zu hinterlegen und an einem sicheren Ort zu verwahren.

- Vor Rückgabe und Wiederverwendung dienstlicher USB-Datenträger sind darauf gespeicherte Daten mit Personenbezug zu löschen. Nicht mehr benötigte oder beschädigte digitale Datenträger (z. B. Festplatten, USB-Sticks oder DVDs), auf denen personenbezogene Daten elektronisch, magnetisch oder optisch gespeichert sind oder waren, sind gemäß den Maßnahmenempfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu entsorgen.

[13] Siehe Dienstanweisung für die Nutzung der Schulverwaltungsrechner im Landesnetz Bildung (LanBSH) des MBWK, veröffentlicht am 03.07.2017.

5.1.6 Server und zentrale Speicherlösungen

Die zentrale Datenablage ist mit der zunehmenden Verarbeitung personenbezogener Daten an der [Name der Schule] zu einem wichtigen Bestandteil der IT geworden. Durch die zentralen Speicherlösungen sollen Informationen innerhalb der Schule jederzeit, an jedem Ort und für unterschiedliche Anwendungsszenarien verfügbar sein.

In der einfachsten Form handelt es sich dabei um einen Netzwerk-Ordner, der von allen Arbeitsplätzen der [Name der Schule] innerhalb des Verwaltungs- oder pädagogischen Netzwerks aus erreichbar ist. Im pädagogischen Netzt kann er als Austauschmedium, über das die Lehrkräfte zum Beispiel Dateien verteilen und einsammeln können, fungieren. In einer erweiterten Form bietet die zentrale Datenablage die Möglichkeit, passwortgeschützte Klassenordner einzurichten, sodass der Zugang nur den zugeordneten Benutzerinnen und Benutzern möglich ist. Eine weitere Differenzierung ergibt sich durch die Option, persönliche Ordner anzulegen, sodass jeder Benutzer, jede Benutzerin über einen nur persönlich zugänglichen Speicherbereich verfügt.

Als Datenablage innerhalb der Schulverwaltung und zur zentralen Speicherung der Daten der Schulverwaltungssoftware betreiben alle an das Landesnetz Bildung angeschlossenen Schulen einen eigenen Datenserver (Fileserver). Dieser Server ist in der Schule in einem verschließbaren 19“-Wandschrank verbaut, sodass alle Daten sicher in der Schule verwahrt werden. Aus Gründen der Datensicherheit werden die Daten im Server parallel und synchron auf zwei Festplatten gespeichert (RAID 1), sodass beim Ausfall einer Festplatte der Schulbetrieb nicht beeinträchtigt wird. Die Schulverwaltungsserver, die zur zentralen Datenablage verwendet werden müssen, wie alle Computer, in regelmäßigen Abständen erneuert werden. Ausschlaggebend für einen Wechsel sind sowohl das Alter der Hardware als auch das Alter des verwendeten Betriebssystems.

Der Wechsel der Hardware und die Migration der Daten können durch den Schulträger selbst oder durch ausgewählte Dienstleistungsfirmen erfolgen.

Folgende Maßnahmen sollten bei der Verwendung von Servern mit zentralen Speicherlösungen berücksichtigt werden:

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1	Geeignete Aufstellung	Datenserver zur zentralen Datenablage wurde in einem verschließbaren Wandschrank verbaut.	☐ Ja ☐ Nein
2	Rechte- und Rollenkonzepte	Für die zentrale Speicherlösung ist ein Rechte- und Rollenkonzept eingerichtet worden. Nicht benötigte Benutzerkonten werden umgehend deaktiviert.	☐ Ja ☐ Nein
3	Protokollierung	Sämtliche Zugriffe auf die zentralen Speicherlösungen werden protokolliert.	☐ Ja ☐ Nein

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
4	Überwachung und Verwaltung	Um Fehlersituationen und Sicherheitsprobleme erkennen und beheben zu können, werden die zentralen Speicherlösungen überwacht und verwaltet.	☐ Ja ☐ Nein
5	Regelmäßige Datensicherung	Datensicherungen werden in festgelegten Intervallen vorgenommen. Diese regelmäßigen Datensicherungen ermöglichen es, die auf dem Server gespeicherten Daten wiederherzustellen.	☐ Ja ☐ Nein
6	Aufbewahrung von Sicherungs-medien	Werden Datensicherungen auf externen Datenträgern vorgenommen, so erfolgt deren Aufbewahrung an einem sicheren Ort, räumlich getrennt von Serverraum.	☐ Ja ☐ Nein

Tabelle 19: Anforderungen zur Verwendung von Servern mit zentralen Speicherlösungen

5.1.7 Drucker

Drucker, Kopierer, Multifunktionsgeräte und Scanner sind heutzutage oft Server mit eigenem Betriebssystem und mechanischen Komponenten. Die zu druckenden oder gescannten Dokumente werden dabei digital in einem internen Speicher abgelegt. Da die Geräte oft vertrauliche Informationen verarbeiten, müssen sie bzw. die gesamte Druck- und Scan-Infrastruktur geschützt werden.

Für viele Schulprozesse der [Name der Schule] wird auch heute noch Papier als Informationsträger benutzt, damit sind Drucker und Multifunktionsgeräte wichtige Komponenten in der IT-Infrastruktur. Netzwerkdrucker, die nicht direkt mit dem Computer verbunden sind, sondern wie ein eigenständiger Server im Rechnernetz angesprochen werden, haben den Vorteil, dass Dokumente schnell und unkompliziert gedruckt und zu Papier gebracht werden können. Netzwerkdrucker erhöhen aber auch das Risiko eines Fremdzugriffs (z.B. durch Hacker). Schafft es ein Angreifer, sich Zugriff auf einen netzwerkfähigen Drucker zu verschaffen, kann er beispielsweise unbemerkt sämtliche Ausdrucke umleiten oder den Speicher auslesen und damit Zugriff auf sämtliche damit verarbeiteten Dokumente der [Name der Schule] erhalten.

Für einen sicheren Umgang mit Druckern, Multifunktionsgeräten und Scannern sollten die folgenden Maßnahmen berücksichtigt werden:

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1	Aufstellung	Drucker und Multifunktionsgeräte sind so aufgestellt, konfiguriert und abgesichert worden, dass nur befugte Anwender die Geräte benutzen und auf verarbeitete Informationen zugreifen können.	☐ Ja ☐ Nein

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
2	Aktualisierung	Es wird regelmäßig überprüft, ob die Drucker, Kopierer und Multifunktionsgeräte auf dem aktuellen Stand sind (bspw. durch Firmwareupdates).	☐ Ja ☐ Nein
3	Benutzer- und Administrations-richtlinien	Für den sicheren Umgang mit Druckern und Multifunktionsgeräten ist eine Administrationsrichtlinie ausgearbeitet worden. Für die Benutzer ist außerdem ein Merkblatt erstellt worden, auf dem alle Sicherheitsvorgaben zum Umgang mit Druckern und Multifunktionsgeräten übersichtlich und verständlich zusammengefasst sind.	☐ Ja ☐ Nein
4	Einschränkung der Anbindung	Netzdrucker und Multifunktionsgeräte sind nicht aus Fremdnetzen erreichbar. Wenn Multifunktionsgeräte an das Telefonnetz angeschlossen werden, ist sichergestellt, dass keine unkontrollierten Datenverbindungen zwischen dem Datennetz der Institution und dem Telefonnetz aufgebaut werden können.	☐ Ja ☐ Nein
5	Authentisierung und Autorisierung	Es werden nur zentrale Drucker und Multifunktionsgeräte eingesetzt, bei denen sich die Benutzer authentisieren müssen, bevor sie diese benutzen können.	☐ Ja ☐ Nein

Tabelle 20: Anforderungen zum Umgang mit Druckern, Multifunktionsgeräten und Scannern

5.2 Software

5.2.1 Schulverwaltungssoftware

Bei den in Schleswig-Holstein eingesetzten Schulverwaltungsprogrammen handelt es sich vielfach um evolutionär gewachsene Produkte, die den aktuellen Anforderungen vernetzter Schulverwaltungen und den damit verbundenen informationssicherheitstechnischen Auflagen nicht immer in angemessener Weise gerecht werden. Einhergehend mit den Bestrebungen, die im Landesnetz genutzten Verfahren zu vereinfachen und zu standardisieren, wurden durch die AG IT-Schulverwaltung[14] die folgenden Programmstandards entwickelt und wie folgt formuliert:

- „Im Landesnetz Bildung sollen nur Schulverwaltungsprogramme eingesetzt werden, die netzwerkfähig sind, über das Landesnetz installiert werden können, über das Landesnetz aktualisiert werden können und vom Unabhängigen Landeszentrum für Datenschutz zertifiziert worden sind.“ (AG IT-Schulverwaltung, 2009).

- Obwohl die hier genannten Programmstandards noch nicht von allen Softwareherstellern vollständig umgesetzt worden sind, werden im Landesnetz Bildung auch weiterhin alle von Schulen eingesetzten Schulverwaltungsprogramme durch den Helpdesk technisch betreut. Außerdem kann das IQSH die Schulen bei der Wahl eines geeigneten Schulverwaltungsprogrammes beraten.

- Mit der Einführung der einheitlichen Schulverwaltungssoftware wird zukünftig eine zentrale Anwendung, die die datenschutzrechtlichen Anforderungen und die Anforderungen an die Datensicherheit erfüllt, zur Verfügung stehen.

Die Schulverwaltungssoftware darf nur auf Schulverwaltungsrechnern installiert werden, die nicht direkt an das Internet angeschlossen werden. Sie sind ausschließlich über das gesicherte LanBSH anzubinden. Die genutzten Schulverwaltungsrechner dürfen nur für dienstliche Zwecke von den dazu berechtigten Nutzerinnen und Nutzern verwendet werden. Dieses Konzept des „Landesnetz Bildung Schleswig-Holstein“ (LanBSH) soll den Schulen Schleswig-Holstein die Aufgabe abnehmen, die Vorgaben und Regeln zur ordnungsgemäßen elektronischen Datenverarbeitung selbst umzusetzen. Mit dem LanBSH erhalten die Schulen Schleswig-Holsteins nicht nur nach dem Stand der Technik sicher konfigurierte PCs für Ihre Schulverwaltung. Durch die Anbindung der Rechner an das Landesnetz ist zudem eine sichere Internetanbindung gewährleistet. Da alle im LanBSH eingebundenen Schulen Mitglied in einer eigenen Benutzergruppe innerhalb des Landesnetzes sind, ist ein relativ sicheres Versenden und Empfangen von E-Mails von Schule zu Schule möglich, da die E-Mail nicht über das Internet, sondern innerhalb des LanBSH transportiert wird. Damit wird weitgehend sichergestellt, dass die Inhalte solcher E-Mails nicht durch Unbefugte eingesehen werden können. Somit können die Schulen Schleswig-Holsteins grundsätzlich auch personenbezogene Daten von Schule zu Schule und mit anderen öffentlichen Stellen austauschen, ohne weitere Sicherheitsvorkehrungen treffen zu müssen (siehe auch Kapitel 5.4.1).

[14] Bei der AG IT-Schulverwaltung handelt es sich um eine gemeinsame Arbeitsgruppe des Ministeriums für Schule und Berufsbildung und der kommunalen Landesverbände.

Die Schulverwaltungssoftware ist hauptsächlich nach den im Schulalltag notwendigen Verwaltungsabläufen konfiguriert. Änderungen an den Einstellungen des Betriebssystems und der Anwendungsprogramme sowie das Hinzufügen oder Löschen von Programmen ist nur von der Schulleitung oder dem beauftragten Administrator gestattet.

Die Schulverwaltungsrechner im Landesnetz sind entsprechend aktuell geltenden Empfehlungen für die schulische IT- und Medienausstattung in Schleswig-Holstein auszustatten:

- Betriebssystem (Windows);
- Schulverwaltungsprogramm(e);
- Technische Anbindung an den Schulträger;
- Büro-Software (Microsoft Word, Excel, PowerPoint, Outlook und Adobe Reader);
- E-Mail-Programm (Microsoft Outlook);
- System-Webbrowser (Microsoft);
- Antivirenprogramme.

5.2.2 Verschlüsselung von Datenbeständen

Um sicherzustellen, dass elektronisch gespeicherte personenbezogenen Daten die auf Speichermedien und Speichersystemen der [Name der Schule] abgelegt sind nicht von Unbefugten eingesehen oder verändert werden können, empfiehlt es sich, diese Daten zu verschlüsseln. Hierfür gibt es verschiedenste Programme.

Für die Verschlüsselung von Einzeldateien kann das Programm AxCrypt verwendet werden, welches kostenfrei als OpenSource-Produkt angeboten wird[15].

Das IQSH stellt eine Verschlüsselungslösung zum Download bereit, die speziell auf USB-Sticks zugeschnitten ist, und keine Installation des Programms auf dem eigenen Rechner erfordert.[16]

5.2.3 Backups/Datensicherung

Regelmäßige Datensicherungen sind erforderlich, um Datenverluste im Falle des Ausfalls des Systems durch technische Defekte oder des Diebstahls des Rechners vorzubeugen. Es sind Regelungen zu treffen, welche Daten von wem wann gesichert werden. Empfehlenswert ist die Erstellung eines Datensicherungskonzeptes.

Die Abstände, in denen Datensicherungen vorgenommen werden sollten, sind dabei abhängig von der Intensität der Änderungen der Datenbestände. So kann es beispielsweise in einer Schule mit wenigen Schülerinnen und Schülern ausreichen, eine Datensicherung nur

[15] Download im Bildungsportal: https://za.schleswig-holstein.de/zentralsek2/axcrypt.php oder auf der Entwicklerseite: https://www.axcrypt.net/download/

[16] https://fit.lernnetz.de/doku.php?id=themen:mobiler-datensafe
Entwicklerseite VeraCrypt: https://www.veracrypt.fr/en/Downloads.html

einmal wöchentlich durchzuführen. In der Regel sollten aber täglich Backups der Daten erfolgen.

Grundsätzlich ist zu beachten, dass die Sicherungsmedien nicht in der Nähe des Rechners aufbewahrt werden. Die Datensicherungsmedien sollten in jedem Fall in einem anderen Raum gelagert werden. Die Aufbewahrung sollte in einem Tresor oder einem speziellen Datensicherungsschrank erfolgen. Sind solche Behältnisse nicht vorhanden, kann die Sicherung auch in einem abschließbaren Schrank verwahrt werden.

Das IQSH hat Hinweise für die Datensicherungen von LanBSH-Rechnern herausgegeben.[17]

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1	Sensibilisierung	Das Sekretariatspersonal und die Lehrkräfte wurden über die Regelungen zur Datensicherung informiert.	☐ Ja ☐ Nein
2	Aufbewahrung – verschiedene Räume	Die Datensicherungsmedien und die Rechner werden nicht in dem selben Raum gelagert.	☐ Ja ☐ Nein
3	Aufbewahrung – abschließbare Schränke	Die Datensicherungsmedien werden in einem abschließbaren speziellen Datensicherungsschrank aufbewahrt.	☐ Ja ☐ Nein
4	Backups	Es werden regelmäßige automatische Backups der Datenbestände durchgeführt.	☐ Ja ☐ Nein

Tabelle 21: Anforderungen zur regelmäßigen Datenabsicherung

5.2.4 Passwörter

Schulverwaltungsrechner und die dazugehörige Schulverwaltungssoftware die innerhalb des „Landesnetz Bildung Schleswig-Holstein“ (LanBSH) verwendet werden müssen mit einer Zugangssicherung ausgestattet sein. Das bedeutet, dass Benutzerinnen oder ein Benutzer eines Schulverwaltungsrechners sich mindestens mit einem Login und einem Passwort identifizieren müssen. Voraussetzung hierfür ist, dass das verwendete Betriebssystem eine solche Zugangssicherung anbietet. Für Microsoft-Betriebssysteme, die laut Dienstanweisung für Schulverwaltungsrechner für die Schulen Schleswig-Holsteins zulässig sind, ist diese Zugangssicherung der Standard.

Nach aktuellem Stand gelten mindestens achtstellige Passwörter als relativ sicher. Dies gilt jedoch nur, wenn sie aus einer Kombination von Buchstaben, Zahlen und Sonderzeichen gebildet werden. Einfache Passwörter können schnell und unkompliziert durch Wörterbuch-

[17] Siehe IT Ausstattungsempfehlung 2015 des IQSH, Abschnitt 5.2., veröffentlicht im August 2015.

oder Brute-Force-Attacken ermittelt werden[18]. Weitere Vorgaben zur Festlegung eines Passworts finden sich ebenfalls in der Dienstanweisung für Schulverwaltungsrechner.[19]

Die Schulleitung ist dafür zuständig das Sekretariatspersonal und die Lehrkräfte der [Name der Schule] dafür zu sensibilisieren, die Standards zur Festlegung sicherer Passwörter einzuhalten, sofern die Einhaltung der Passwortrichtlinie nicht bereits im System implementiert ist.

Zur Festlegung der Passwörter sollten folgende Maßnahmen berücksichtigt werden:

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1	Verwaltung der Benutzer	Sämtliche Benutzerinnen und Benutzer des Landesnetzes Bildung sind im Verzeichnisdienst des Landes verwaltet. (Die Administration erfolgt im Regelfall durch das IQSH oder durch Schulträger, die die Benutzerverwaltung ihrer Schulen verantwortlich übernommen haben.)	☐ Ja ☐ Nein
2	Benutzername und Passwort	Jede im Verzeichnisdienst als berechtigt registrierte Person meldet sich mit ihrem individuellen Benutzernamen und dem zugehörigen Passwort für die Nutzung des Schulverwaltungsrechners an.	☐ Ja ☐ Nein
3	Kennwortlänge und Zusammensetzung	Das Startpasswort für die erste Anmeldung ist vorgegeben. Jede Benutzerin und jeder Benutzer erstellt danach ein neues Passwort für sich selbst. Es muss mindestens aus acht Zeichen bestehen. Aufgrund der Passwortrichtlinie müssen darin jeweils mindestens ein Buchstabe, eine Zahl und mindestens ein Sonderzeichen enthalten sein.	☐ Ja ☐ Nein
4	Keine „einfachen“ Passwörter	Passwörter mit spezieller, von Außenstehenden leicht zu erratender Bedeutung, wie Namen, Geburtsdaten, Firmen- oder Abteilungs-bezeichnungen, Kfz-Kennzeichen etc. sowie Standardausdrücke wie TEST,SYSTEM und Tastatur- und Zeichenmuster, wie ABCDEF, QWERTZ, 123456 etc. werden nicht als Passwort verwendet.	☐ Ja ☐ Nein
5	Voreingestellte Passwörter	Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) werden umgehend durch individuelle Passwörter ersetzt. Der Hersteller bzw. Lieferant sollte dazu nach allen voreingestellten Benutzerkennungen und Passwörtern befragt werden.	☐ Ja ☐ Nein

[18] Bei Wörterbuch-Attacken werden die Einträge von Wörterbüchern automatisiert als Passwort ausprobiert, um ein Passwort zu ermitteln. Als Erweiterung werden bei der Brute-Force-Attacke alle Zahlen und Buchstaben-Kombinationen automatisiert ausprobiert.

[19] Siehe Dienstanweisung für die Nutzung der Schulverwaltungsrechner im Landesnetz Bildung (LanBSH) des MBWK, veröffentlicht am 03.07.2017.

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
6	Programmierbare Funktionstasten	Passwörter werden nicht auf programmierbaren Funktionstasten gespeichert.	☐ Ja ☐ Nein
7	Unbeobachtete Eingabe	Die Eingabe des Passwortes wird unbeobachtet durchgeführt.	☐ Ja ☐ Nein
8	Verdeckte Anzeige auf dem Bildschirm	Bei der Eingabe wird das Passwort nicht im Klartext angezeigt (Bsp.: Verdeckt durch Sternsymbol).	☐ Ja ☐ Nein
9	Geheimhaltung des Passworts	Das Passwort wird geheim gehalten und wird nur den jeweiligen Nutzenden persönlich bekannt gegeben.	☐ Ja ☐ Nein
10	Schriftliche Fixierung	Das Passwort wird nicht schriftlich fixiert.	☐ Ja ☐ Nein
11	Regelmäßige Passwortänderungen	Das Passwort wird regelmäßig gewechselt, z. B. alle 90 Tage.	☐ Ja ☐ Nein
12	Sofortiger Passwortwechsel	Ist das Passwort unautorisierten Personen bekannt geworden, so wird ein sofortiger Passwortwechsel durchgeführt.	☐ Ja ☐ Nein
13	Sperrbildschirm	Auf jedem Schulverwaltungsrechner ist ein Sperrbildschirm mit Passwortschutz eingerichtet. Er wird nach spätestens 10 Minuten ohne Aktivität am Computer automatisch eingeschaltet. Diese Einstellung ist vorgegeben und nicht veränderbar. Bei Verlassen des Arbeitsplatzes − auch bei kurzfristiger Abwesenheit − ist der Computer zu sperren, d. h. der Sperrbildschirm ist zu aktivieren (z. B. durch Drücken der Tastenkombination „Windows-Taste + L“).	☐ Ja ☐ Nein
14	Verzögerter Login	Bei einem fehlerhaft eingegebenen Passwort verzögert sich die Möglichkeit des erneuten Anmeldevorganges systemseitig um min. 1 Sekunde, um Brute-Force-Attacken entgegenzuwirken	☐ Ja ☐ Nein

Tabelle 22: Anforderungen zur Festlegung von Passwörtern

5.2.5 Umgang mit Nicht-Verwaltungssoftware

Die Verwendung von zusätzlicher Nicht-Verwaltungssoftware ist grundsätzlich nicht zulässig. Zur Freigabe weiterer benötigter Software, insbesondere für den pädagogischen Bereich wenden Sie sich bitte an das MBWK oder Ihren Ansprechpartner des IQSH.

5.2.6 Nutzung von Standardsoftwareprodukten

Allgemein bezeichnet der Begriff Standardsoftware die Software, die auf dem Markt angeboten und meistens über den Fachhandel bezogen wird, zum Beispiel über Kataloge oder Onlineportale. Sie ist dadurch gekennzeichnet, dass Institutionen sie selbst installieren und mit wenig Aufwand anpassen können.

Im Schulbereich ist hier insbesondere die Software, die laut Dienstanweisung Schulverwaltungsrechner im Landesnetz Bildung vorgegeben wird, zu nennen:

- Betriebssystem (Windows);
- Schulverwaltungsprogramm(e), z.B. WinSchool, Scola, Untis etc.;
- Technische Anbindung an den Schulträger;
- Büro-Software (Microsoft Word, Excel, PowerPoint, Outlook und Adobe Reader);
- E-Mail-Programm (Microsoft Outlook);
- System-Webbrowser (Microsoft);
- Antivirenprogramme.

Die Schulverwaltungsrechner sind dabei so konfiguriert, dass sie die rechtlichen Vorgaben und die im Schulalltag notwendigen Verwaltungsabläufe eingehalten werden können. Das bedeutet für die Standardsoftware, dass Änderungen, Hinzufügen oder Löschen an den Einstellungen des Betriebssystems und der Anwendungsprogramme nur von der Schulleitung durch einen schriftlich beauftragten Administrator in Übereinstimmung mit dem IT- und Sicherheitskonzept durchgeführt werden darf. Die Verwendung von Cloud-Angeboten[20] privater Dienstleister ist generell unzulässig.

Für die eingesetzten Schulverwaltungsprogramme sind bei Installation und Betrieb die Maßgaben gemäß den Anleitungen der Hersteller zu beachten.

[20] Die Anbieter von Cloud-Diensten speichern die Daten der Nutzenden in der Regel unter nicht offengelegten Bedingungen auf nicht näher bestimmten Servern, so dass die Nutzenden keine Kontrolle über ihre Daten haben. Im Gegensatz dazu werden bei einer Auftragsverarbeitung (siehe § 12 SchulDSVO) mit dem jeweiligen Dienstleister die Konditionen der Datenverarbeitung vertraglich festgelegt und mit Umsetzung der relevanten Vorschriften (u. a. Verfahrensdokumentation) wird ein datenschutzkonformer Ablauf sichergestellt.

Zur sicheren Anwendung von Standardsoftwareprodukten werden folgende Maßnahmen empfohlen:

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1	Installation	Bei der Installation von Standardsoftwareprodukten ist sichergestellt, dass nur freigegebene Originalsoftware verwendet wird. Für die eingesetzten Standardsoftwareprodukte wird eine an den Bedarf der Schule angepasste Standardkonfiguration erstellt und genutzt. Diese Konfiguration wird in einer Installations- und Konfigurationsanweisung dokumentiert.	☐ Ja ☐ Nein
2	Versionskontrolle	Es wird eine regelmäßige Kontrolle der installierten Versionen von Standardsoftwareprodukten durchgeführt. Diese Bestandsführung der Software-Lizenzen wird bei jeder Installation oder Deinstallation aktualisiert.	☐ Ja ☐ Nein
3	Updates	Updates zu Standardsoftwareprodukten werden ausschließlich aus sicheren Quellen bezogen. Bestenfalls vom Hersteller der Software.	☐ Ja ☐ Nein
4	Aktive Inhalte	Das automatische Ausführen von eingebetteten aktiven Inhalten, wie beispielsweise Makros oder ActiveX-Elemente, werden in den Einstellungen aller verwendeten Office-Produkte deaktiviert. Ist die Ausführung aktiver Inhalte für einen Schulprozess notwendig, dann wird darauf geachtet, dass nur aktive Inhalte von vertrauenswürdigen Quellen ausgeführt werden.	☐ Ja ☐ Nein
5	Öffnen von Dokumenten aus externen Quellen	Alle aus externen Quellen bezogenen Dokumente werden vor dem Öffnen auf Schadsoftware überprüft. Alle als problematisch eingestuften Dateiformate sind verboten.	☐ Ja ☐ Nein
6	Auswahl geeigneter Standardsoft-wareprodukte	Für die Beschaffung von Standardsoftwareprodukten werden die Anforderungen der Schule durch die Schulleitung erhoben. Diese sollten in einem Anforderungskatalog dokumentiert werden.	☐ Ja ☐ Nein
7	Testen neuer Versionen	Neue Versionen von Standardsoftwareprodukten werden vor dem Einsatz in der Schule auf Kompatibilität mit etablierten Arbeitsmitteln (z. B. Dokumentenvorlagen, Formularen) der Schule geprüft.	☐ Ja ☐ Nein

Tabelle 23: Anforderungen zur Anwendung von Standardsoftwareprodukten

5.2.7 Antivirus/Firewall

In den dezentralen Netzen liegt die Verantwortung für einen funktionsfähigen und stets aktuellen Schutz vor Schadprogrammen bei der Schulleitung und dem Schulträger gleichermaßen.

Unter Computerviren versteht man allgemein „Programme mit Schadensfunktionen“. Dies sind Anwendungen, die verdeckte Funktionen enthalten und damit durch Löschen, Überschreiben oder sonstige Veränderungen unkontrollierbare Schäden an Programmen und Daten bewirken können. Damit verursachen sie zusätzliche Arbeit und Kosten und schaden der Vertraulichkeit, Integrität und Verfügbarkeit von Daten oder Software.

In der folgenden Tabelle werden einige Programme mit Schadensfunktionen beschrieben:

Name	Beschreibung
Viren	Nichtselbstständige, in anderen Programmen oder Dateien eingebettete Programmroutinen, die sich selbst reproduzieren und dadurch nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornehmen.
Trojanische Pferde	Selbständige Programme mit verdeckter Schadensfunktion, ohne Selbstreproduktion. Trojanische Pferde dienen vor allem dazu, Computer auszuspionieren.
Logische Bomben	Programme, deren Schadensfunktion von einer logischen Bedingung gesteuert wird, beispielsweise dem Datum oder einer bestimmten Eingabe.
Würmer	Selbständige, selbstreproduzierende Programme, die sich in einem System (vor allem in Netzwerken) ausbreiten.

Tabelle 24: Programme mit Schadenfunktionen

Das nachfolgende Kapitel beschäftigt sich vorwiegend mit dem Schutz gegen Viren und Würmer, die zur Vereinfachung im Folgenden generell als „Viren“ bezeichnet werden. Die angeführten Maßnahmen sind überwiegend auch gegen andere Arten von Software mit Schadensfunktion, wie z. B. Trojanische Pferde anwendbar.

Um einen Virenbefall so weit wie möglich vorzubeugen, bzw. im Falle eines Virenbefalls den Schaden möglichst zu begrenzen sollten die Schulen sowohl technische als auch organisatorische Schutzmaßnahmen einführen.

Die nachfolgenden Maßnahmen geben eine Reihe von generellen Empfehlungen zum Virenschutz, die an die Erfordernisse der betroffenen Schulen anzupassen sind. Je mehr bzw. je exakter die Empfehlungen umgesetzt werden, desto geringer wird das allgemeine Risiko:

- Regelmäßige Durchführung einer Datensicherung;
- Sichere Aufbewahrung der Sicherheitskopien;

- Setzen eines Schreibschutzes bzw. Nutzung von nur einmal beschreibbaren Medien bei allen Datenträgern, auf die nicht geschrieben werden muss (gilt insbesondere für Datenträger, die Programme beinhalten) und bei allen ausgehenden Datenträgern;
- Überprüfung aller ein- und ausgehenden Datenträger die in das Endgerät eingesteckt werden;
- Überprüfung aller vorinstallierten Neugeräte und Geräte;
- Es sollten nur vertrauenswürdige Programme zugelassen sein, die auch über entsprechende Sicherheitsfunktionen verfügen. Dies gilt in besonderem Maße für E-Mail-Programme. Für Probleme sollten zentrale Ansprechstellen (E-Mail-Adresse, Telefon und Fax-Nummer) benannt werden.

Das Risiko eines Virenbefalls lässt sich durch die Installation und Nutzung von Firewall- und Antivirenprogrammen verringern, die im Fachhandel erhältlich sind. Für die Auswahl geeigneter Firewall- und Antivirenprogramme sollte zusätzlich die fachliche Expertise des IQSH eingeholt werden.

Abschließend werden in der folgenden Tabelle die Maßnahmen aufgelistet, die zum Schutz vor Schadprogrammen durchgeführt werden sollten:

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1	Systemspezifische Schutz-mechanismen	Es wurde geprüft, welche Schutzmechanismen die verwendeten IT-Systeme sowie die darauf genutzten Betriebssysteme und Anwendungen bieten, um einen Schutz vor Schadprogrammen zu ermöglichen bzw. zu unterstützen.	☐ Ja ☐ Nein
2	Auswahl des Schutzprogramms	In Abhängigkeit vom verwendeten Betriebssystem, anderen vorhandenen Schutzmechanismen ist ein geeignetes Schutzprogramm ausgewählt und installiert worden.	☐ Ja ☐ Nein
3	Betrieb von Schutz-programmen	Das Schutzprogramm ist für seine Einsatzumgebung geeignet konfiguriert worden (bspw. regelmäßige automatische Überprüfungen/Scans von Dateien).	☐ Ja ☐ Nein
4	Aktualisierung von Schutzprogrammen	Auf den damit ausgestatteten IT-Systemen werden die Viren-Schutzprogramm regelmäßig aktualisiert.	☐ Ja ☐ Nein
5	Sensibilisierung der Benutzer	Die an der Schule tätigen Personen werden regelmäßig über die Bedrohung durch Schadprogramme aufgeklärt. Sie halten die grundlegenden Verhaltensregeln ein, um die Gefahr eines Befalls durch Schadprogramme zu reduzieren. Dateien aus nicht vertrauenswürdigen Quellen werden nicht geöffnet.	☐ Ja ☐ Nein

Tabelle 25: Maßnahmen zum Schutz vor Schadprogrammen

5.4 Kommunikation

5.4.1 E-Mail

Die E-Mail-Kommunikation darf bei Nutzung eines Landesnetzrechners nur über ein persönliches E-Mail-Postfach im Landesnetz (z.B. Maren.Muster@schule.landsh.de) stattfinden. Das Postfach darf nur dem jeweiligen Schulpersonal zugänglich sein und ist ausschließlich für dienstliche Zwecke zu verwenden. Das Versenden von vertraulichen Informationen oder personenbezogenen Daten per E-Mail ist grundsätzlich nur innerhalb des Landesnetzes zulässig. Im Falle des Ausscheidens des Schulpersonals aus der Schule, ist die Löschung des Postfaches unverzüglich beim IQSH Helpdesk zu beauftragen.

Zum Zwecke der Speicherung und Dokumentation von aktenrelevanten E-Mails sind diese auszudrucken und in Papierform der jeweiligen Akte beizulegen. Nach diesem Vorgang sind E-Mails mit personenbezogenen Inhalten gemäß den Vorgaben nach §10 Abs.1 SchulDSVO zu löschen, sobald sie nicht mehr für die konkrete Aufgabenerfüllung des Schulpersonals erforderlich sind und der zugehörige Vorgang abgeschlossen ist.

Im „Outlook-Adressbuch“ sind bereits Adressdaten aller im Landesnetz registrierten Nutzerinnen und Nutzer gespeichert. Das Hinzufügen dienstlich erforderlicher E-Mail-Adressen der Betroffenen ist in „Outlook-Kontakte“ möglich. Kommuniziert die Schule mit Eltern, Schülerinnen und Schülern oder Lehrkräften mithilfe von E-Mail-Adresslisten, können diese in „Outlook-Kontakte“ eingerichtet werden. Es ist in diesem Fall sicherzustellen, dass sich diese E-Mail-Adressen immer auf dem aktuellen Stand befinden. Über die Kontaktdaten hinausgehende Informationen sind ausschließlich im Schulverwaltungsprogramm zu verarbeiten. Dienstlich erforderliche Adressdaten einschließlich E-Mail-Adressen und Telefonnummern von öffentlichen und nichtöffentlichen Stellen, die für die Schulverwaltung zur Aufgabenerfüllung erforderlich sind, dürfen in „Outlook-Kontakte“ gespeichert werden.

Bei einer E-Mail, die gleichzeitig an mehrere Adressen versendet wird, sind die E-Mail-Adressen zum Schutz der Empfängerinnen und Empfänger gegenseitig zu verbergen und ausschließlich über die „BCC“-Funktion einzufügen. In das „An“-Feld ist die Adresse des Absenders (z. B. Musterschule. Ort@schule.landsh.de) aufzunehmen.

Zur Sicherheit des gesamten Landesnetzes sind eingegangene E-Mails mit eindeutig nicht dienstlichem Bezug (z. B. Werbemails und Spam) oder E-Mails mit der Aufforderung zur Eingabe von Benutzerdaten und Passwörtern (Phishing-Angriff) zu ignorieren und unverzüglich endgültig zu löschen. Unerwartet und unaufgefordert eingegangene E-Mails, die mit ausführbaren Anhängen oder unspezifisch benannten Dateien versehen sind, sind ebenfalls unverzüglich zu löschen. Ausnahmen bilden E-Mails, deren Identität des Absenders und dessen Integrität sowie die des Inhalts der E-Mail durch eine Überprüfung (beispielsweise eine persönliche Rückversicherung beim Absender) eindeutig und zweifelsfrei bestätigt werden konnten.

Der ULD Schleswig-Holstein hat zur E-Mail-Nutzung darüber hinaus folgende Hinweise herausgegeben[21]:

Teil 1: Versenden von E-Mails

1. Der Betreff:
    - Verwenden Sie immer eine Betreffzeile;
    - Der Betreff sollte kurz und aussagekräftig sein, idealerweise den Inhalt der Nachricht bzw. die Thematik kurz umreißen.

Warum? Zum einen erleichtert eine kurze, klare Betreffzeile dem Empfänger/-in die Abarbeitung der E-Mail. Er/Sie kann schnell entscheiden, in welchen Kontext diese gehört und kann sie entsprechend bearbeiten. Zum anderen wird durch eine aussagekräftige Betreffzeile deutlich, dass es sich nicht um eine automatisch generierte Nachricht eines Mailwurms handelt. Diese verwenden häufig nur pauschale Betreffzeilen wie „Hi!" oder „Ihre Anfrage".

2. Der Text:
    - Verwenden Sie immer eine direkte Ansprache des Empfängers;
    - Erwähnen Sie immer eventuell beigefügte Anhänge: „Anbei übersende ich Ihnen…".

Warum? Auch die direkte Anrede macht klar, dass die Nachricht mit hoher Wahrscheinlichkeit nicht von einem E-Mailwurm stammt. Anhänge, die Sie einer E-Mail beifügen, sollten Sie als solche auch kenntlich machen. Andernfalls könnte der Verdacht entstehen, der Anhang sei durch einen Wurm erzeugt und der Mail automatisch beigefügt.

3. Der Anhang:
    - Vermeiden Sie Anhänge, wenn es geht. Einfache Texte ohne Formatierungen können ebenso gut direkt in die E-Mail kopiert werden.
    - Versenden Sie nur potentiell sichere Dokumenttypen (bspw. PDF).
    - Versenden Sie Word-Dokumente nur im Ausnahmefall und nur auf ausdrücklichen Wunsch des Empfängers!

Warum? Durch die Vermeidung eines Anhangs ersparen Sie dem Empfänger nicht nur Zeit (er muss kein separates Programm zum Betrachten starten), sondern auch die Mühe zu entscheiden, ob er Ihrem Anhang traut und ihn öffnet. Durch das Verwenden potenziell sicherer Formate wie PDF, setzen Sie ein klares Zeichen für den Empfänger: Diese E-Mail enthält keinen Wurm oder Virus. Bei Word-Dokumenten gilt besondere Vorsicht. Dabei sind eventuell enthaltene Makroviren nur eine mögliche Gefahr. Ein anderes Risiko stellen in Word-Dokumenten enthaltene Revisionsinformationen dar. Das können die letzten

[21] Siehe Praxishandbuch Schuldatenschutz des ULD Schleswig-Holstein, S.207, veröffentlicht im Jahre 2009.

Änderungen sein oder auch Kommentare von Ihnen oder von Mitautoren. Aus diesem Grund sollten Word-Dokumente vor dem Versenden in PDF umgewandelt werden.

Teil II: Empfang von E-Mails

1. Der Betreff
    - Ist der Betreff sinnvoll?
    - Ist der Betreff in der vom Absender gewohnten Sprache?
    - Hat der Betreff einen Bezug zu dienstlichen Themen und Aufgaben?

Warum? Automatisch generierte Nachrichten von E-Mail-Würmern enthalten häufig allgemeine Betreffzeilen, die entweder inhaltsleer sind („Hi!") oder die Aufmerksamkeit des Empfängers erwecken sollen („Bilder von der letzten Party"). Da viele E-Mail-Würmer aus dem englischsprachigen Raum stammen, sind häufig die Betreffzeilen ebenfalls englisch. Daher sollte eine englische Betreffzeile von einem deutschen Absender zumindest zur Vorsicht animieren.

2. Der Text:
    - Hat die E-Mail einen Textteil?
    - Werden Sie als Empfänger persönlich angesprochen?
    - Ist der Text in der vom Absender gewohnten Sprache?
    - Ist der Text im vom Absender gewohnten Sprachstil?
    - Wird ein beigefügter Anhang im Text erwähnt?

Warum? Auch hier geht es darum, automatisch erzeugte E-Mails zu enttarnen. Eine fehlende Anrede oder gar kein E-Mailtext deuten auf z.B. auf E-Mail-Würmer hin. Auch die Sprache der E-Mail ist wichtig. Schreibt ein deutscher Absender plötzlich englische E-Mails, ist Vorsicht geboten. Es könnte sein, dass er die E-Mail nicht selbst verfasst hat. Ebenso, wenn der Sprachstil sich signifikant unterscheidet.

3. Der Anhang:

- Wird der Anhang vom Absender erwartet? (Erwähnung im E-Mail-Text, per Telefon oder auf anderem Wege angekündigt);
- Handelt es sich um ein Dokument oder ein Programm?

Warum? E-Mails, die überraschende Anhänge enthalten, sind verdächtig. Niemand hängt eine Datei an eine E-Mail, ohne darüber ein Wort der Erklärung zu verlieren. Wenn ein Anhang einer E-Mail beigefügt wurde, überprüfen Sie unbedingt, um welchen Typ von Datei es sich handelt, bevor sie darauf klicken.

Zusammenfassend lassen sich somit die folgenden Maßnahmen für den sicheren E-Mail-Umgang zusammenfassen:

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1	E-Mail Kommunikation im Landesnetz	Die E-Mail Kommunikation wird bei Nutzung eines Landesnetzrechners nur über ein persönliches E-Mail-Postfach im Landesnetz durchgeführt.	☐ Ja ☐ Nein
2	Zugang zum Schul-Postfach	Das Schul-Postfach als nicht personalisierte Behördenadresse ist nur für das jeweilige Schulpersonal zugänglich und wird nur für dienstliche Zwecke verwendet.	☐ Ja ☐ Nein
3	Versenden von personenbezo-genen Daten	Das Versenden von vertraulichen Informationen oder personenbezogenen Daten per E-Mail wird grundsätzlich nur innerhalb des Landesnetzes durchgeführt. E-Mails mit personenbezogenen Daten an externe Empfänger sind zu verschlüsseln bzw. die Informationen in verschlüsselten Anhängen zu versenden.	☐ Ja ☐ Nein
4	Verlassen von Schulpersonal	Bei Verlassen des Schulpersonals aus der Schule, wird die Löschung des Postfaches unverzüglich beim IQSH Helpdesk beauftragt.	☐ Ja ☐ Nein
5	Dokumentation von E-Mails	Aktenrelevante E-Mails werden ausgedruckt und in Papierform der jeweiligen Akte beigelegt.	☐ Ja ☐ Nein
6	Löschung von E-Mails mit personenbezo-genen Inhalten	Nach Ablage der E-Mails in Papierform werden E-Mails mit personenbezogenen Inhalten gemäß der Vorgaben nach §10 Abs. 1 SchulDSVO gelöscht, sobald sie nicht mehr für die konkrete Aufgabenerfüllung des Schulpersonals erforderlich sind.	☐ Ja ☐ Nein
7	Aktuelle E-Mail-Adressen	Die E-Mail-Adressen von Eltern, Schülerinnen und Schülern oder Lehrkräften, die mithilfe von E-Mail-Adresslisten versendet werden, sind immer auf dem neuesten Stand.	☐ Ja ☐ Nein
8	E-Mail Kommunikation mit mehreren Empfängern	Bei einer E-Mail, die gleichzeitig an mehrere Adressen versendet wird, werden die E-Mail-Adressen zum Schutz der Empfängerinnen und Empfänger gegenseitig verborgen und ausschließlich über die „BCC“-Funktion eingefügt.	☐ Ja ☐ Nein
9	Versenden von E-Mails	Die Hinweise (Betreff, Text und Anhang) für das Versenden von E-Mails werden berücksichtigt.	☐ Ja ☐ Nein

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
10	Empfang von E-Mails	Die Hinweise (Betreff, Text und Anhang) für den Empfang von E-Mails werden berücksichtigt.	☐ Ja ☐ Nein

Tabelle 26: Anforderungen zum sicheren E-Mail-Umgang

5.4.2 Datenaustausch

Zum Datenaustausch von Schulpersonal, welches in einer Schule tätig ist und somit Schulrechner im Landesnetz verwendet, wird vorgeschrieben, dass ein gesonderter Tauschordner auf dem Server der Schule einzurichten und zu verwenden sind. Zur regelmäßigen Datensicherung unterstützt das IQSH die Schulen mit einem standardisierten und automatisierten Datensicherungsverfahren. Dabei werden die auf dem Fileserver der Schule vorhandenen Daten täglich (in der Nacht) auf ein externes Speichermedium (USB-Festplatte) gespeichert. Die weitere Absicherung des Datenaustauschs untereinander erfolgt dann im gesicherten Landesnetz.

Die schulische Nutzung von Cloud-Diensten (Office 365 u.a.) ist datenschutzrechtlich unzulässig. Die Schulleitung ist für die Einhaltung dieser Regelungen verantwortlich. Dienste, bei denen personenbezogene Daten außerhalb der Schule durch andere, insbesondere nicht-öffentliche Stellen, im Auftrag der Schule verarbeitet werden (Online-Angebote, Lernplattformen u.a.), dürfen nur nach Genehmigung durch das für Bildung zuständige Ministerium und Vorliegen eines Auftragsverarbeitungsvertrages zwischen Auftragnehmer (Anbieter) und Auftraggeber (Schule) in Anspruch genommen werden (§ 12 SchulDSVO). Im Zweifel wenden Sie sich an den zentralen Datenschutzbeauftragten für die öffentlichen Schulen oder das IQSH.

Wechseldatenträger (insbesondere USB-Datenträger) können für erforderliche temporäre Speicherungen dienstlicher Daten (z. B. für die Zeugniserstellung) genutzt werden. Hierfür dürfen ausschließlich dienstlich zur Verfügung gestellte USB-Datenträger verwendet werden. Außerhalb der Schulverwaltung dürfen diese nur mit gemäß § 14 SchulDSVO genehmigten privaten informationstechnischen Geräten der Lehrkräfte verwendet werden. Sofern auf den USB-Datenträgern personenbezogene oder vertrauliche Daten gespeichert sind, sind diese zu verschlüsseln. Die Vergabe des Verschlüsselungspasswortes hat nach den Vorgaben in Kapitel 5.2.4 zu erfolgen. Verschlüsselungspasswörter sind in der Schulverwaltung in einem verschlossenen Umschlag zu hinterlegen und an einem sicheren Ort zu verwahren. Vor Rückgabe und Wiederverwendung dienstlicher USB-Datenträger sind darauf gespeicherte Daten mit Personenbezug zu löschen. Nicht mehr benötigte oder beschädigte digitale Datenträger (z. B. Festplatten, USB-Sticks oder DVDs), auf denen personenbezogene Daten elektronisch, magnetisch oder optisch gespeichert sind oder waren, sind gemäß den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sicher zu entsorgen.

Beim regelmäßigen Datenaustausch mit Dritten ist die Festlegung von Richtlinien bzw. der Abschluss von Vereinbarungen mit allen Beteiligten sinnvoll. Dabei spielt es keine Rolle, wie der Datenaustausch selbst erfolgt (Datenträgeraustausch, E-Mail etc.).

In den Vereinbarungen mit den beteiligten Dritten müssen folgende Punkte enthalten sein:

- Bestimmung der Verantwortlichen;
- Benennung von AnsprechpartnerInnen (in technischen, organisatorischen und sicherheitstechnischen Belangen);
- Festlegung der Datennutzung;
- Welche Anwendungen und Datenformate sind zu verwenden?
- Wie und wo erfolgt die Prüfung auf Virenfreiheit?
- Wann dürfen Daten gelöscht werden?
- Regelung des Schlüsselmanagements, falls erforderlich und
- Einhaltung einschlägiger Gesetze (bspw. SchulG, SchulDSVO, LDSG etc.).

Für den Datenaustausch in der [Name der Schule] sollten folgende Maßnahmen realisiert werden:

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1	Interner Datenaustausch	Für den internen Datenaustausch wird ein gesonderter Tauschordner auf dem Server der Schule eingerichtet und verwendet.	☐ Ja ☐ Nein
2	Regelmäßige Datensicherung	Es findet eine regelmäßige Datensicherung, unterstützt durch das IQSH, statt.	☐ Ja ☐ Nein
3	Cloud-Dienste	Zur schulischen Nutzung werden keine Cloud-Dienste verwendet.	☐ Ja ☐ Nein
4	Wechseldaten-träger	Wechseldatenträger werden ausschließlich für schulische Zwecke verwendet.	☐ Ja ☐ Nein
5	Personenbezo-gene Daten auf Wechseldaten-trägern	Wechseldatenträger auf denen personenbezogene Daten gespeichert sind, werden verschlüsselt.	☐ Ja ☐ Nein
6	Entsorgung von Wechseldaten-trägern	Nicht mehr benötigte oder beschädigte digitale Datenträger (z. B. Festplatten, USB-Sticks oder DVDs), auf denen personenbezogene Daten elektronisch, magnetisch oder optisch gespeichert sind oder waren, werden gemäß der Empfehlungen des Bundesamtes	☐ Ja ☐ Nein

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
		für Sicherheit in der Informationstechnik (BSI) sicher entsorgt.	
7	Datenaustausch mit Dritten	Beim regelmäßigen Datenaustausch mit Dritten werden Richtlinien festgelegt bzw. Vereinbarungen mit allen Beteiligten geschlossen.	☐ Ja ☐ Nein

Tabelle 27: Maßnahmen zum Datenaustausch

5.5 Ordnungsgemäße Administration

Wie bereits in Kapitel 1 beschrieben, ist die Schulleitung der [Name der Schule] dafür verantwortlich, dass die Informationssicherheitsrichtlinien in der Schule eingehalten werden.

Darüber hinaus kann die Schulleitung Ihrer Stellvertreterin/ihrem Stellvertreter oder einer anderen Lehrkraft als Teil einer Aufgabendelegation gem. § 33 Abs. 6 SchulG die Überwachung der Beachtung und Umsetzung der Informationssicherheit und des Datenschutzes in der [Name der Schule] übertragen. Dies entbindet die Schulleitung nicht von der Gesamtverantwortlichkeit nach § 2 SchulDSVO.

Zur Umsetzung der Informationssicherheitsrichtlinien muss die Schulleitung bzw. deren Stellvertreter in der Lage sein, die ordnungsgemäße IT-Administration in der Schule durchzuführen bzw. die Arbeit der Systemadministratorinnen und –administratoren zu überwachen. Die ordnungsgemäße IT-Administration von IT-Systemen und -Komponenten ist für den laufenden IT-Betrieb grundlegend.

Die Systemadministratoren richten dabei IT-Systeme und Anwendungen ein, beobachten den Betrieb und reagieren mit Maßnahmen, die die Funktion und die Leistungsfähigkeit der Systeme der Schule erhalten. Sie passen die Systeme an die veränderten Bedürfnisse an. Dabei erfüllen sie auch eine Reihe von Aufgaben für die IT-Sicherheit: Sie sorgen nicht nur dafür, dass die Systeme verfügbar bleiben, sondern setzen auch Sicherheitsmaßnahmen um und überprüfen, ob sie wirksam sind. Dazu verfügen sie über sehr weitreichende Berechtigungen, sodass es für die Sicherheit der verbundenen IT-Systeme erforderlich ist, die Systemadministration vor unbefugten Zugriffen selbst abzusichern. Zur Aufgabenerfüllung sollten die Systemadministratorinnen und -administratoren der Schule eine enge Zusammenarbeit mit den Ansprechpartnerinnen und -partnern des IQSH anstreben.

Folgende Maßnahmen sollten zur ordnungsgemäßen Administration realisiert werden:

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
1	Personalauswahl	Die Schulmitarbeiter/-innen, die administrative Aufgaben innerhalb der Schule für die IT-Umgebung übernehmen sollen, verfügen über die ausreichende fachliche Qualifikation und erledigen ihre Aufgaben zuverlässig und sorgfältig.	☐ Ja ☐ Nein

Nr.	Name	Beschreibung	Anwendbar (Ja/Nein)
2	Vertretungs-regelungen	Für alle administrativen Verantwortlichkeiten wurden Vertretungsregelungen getroffen. Es ist sichergestellt, dass benannte Vertreter auf die zu betreuenden IT-Systeme zugreifen können.	☐ Ja ☐ Nein
3	Beendigung von Tätigkeiten als IT-Administrator	Wenn Administratorinnen/Administratoren von ihren Aufgaben wieder entbunden werden, werden alle ihnen zugewiesenen persönlichen Administrationskennungen gesperrt.	☐ Ja ☐ Nein
4	Administrations-kennungen	Jedem Administrator/jeder Administratorin und jedem Vertreter/jeder Vertreterin werden eigene, eindeutige Administratorkennungen zugewiesen. Die vergebenen Administrationsrechte sind aus den Erfordernissen der jeweils übernommenen IT-Administrationsaufgaben abzuleiten.	☐ Ja ☐ Nein
5	Schutz administrativer Kennungen	Administrationskennungen werden durch geeignete Authentisierungsmechanismen angemessen geschützt. Werden dafür Passwörter benutzt, dann werden gleichartige Passwörter NICHT für IT-Systeme in anderen Schutzzonen verwendet.	☐ Ja ☐ Nein
6	Regelung der IT-Administrations-tätigkeit	Die Befugnisse, Aufgaben und Pflichten der Administratorinnen und Administratoren sind in einer Arbeitsanweisung oder Richtlinie verbindlich festgeschrieben.	☐ Ja ☐ Nein
7	Ausreichende Ressourcen für den IT-Betrieb	Es werden ausreichende Personal- und Sachressourcen bereitgestellt, um die anfallenden administrativen Aufgaben ordnungsgemäß zu bewältigen. Dabei wurde berücksichtigt, dass auch für unvorhersehbare Tätigkeiten entsprechende Kapazitäten vorhanden sein müssen, insbesondere, um sicherheitsrelevante Ereignisse zu behandeln und aufzuklären.	☐ Ja ☐ Nein
8	Fortbildung und Information	Für die eingesetzten Administratorinnen und Administratoren werden geeignete Fort- und Weiterbildungsmaßnahmen ergriffen, damit sie immer auf dem aktuellen Stand der Technik sind.	☐ Ja ☐ Nein

Tabelle 28: Maßnahmen zur ordnungsgemäßen Administration