IT-Sicherheit und Datenschutz in Schulverwaltungen
Checkliste für Schulleitungen

Vorwort	
Die folgenden Hinweise sollen Schulleitungen als Hilfe dienen, um in ihrem Verantwortungsbereich zu prüfen, ob IT-Sicherheit und Datenschutz ausreihend Beachtung finden und die notwendigen Maßnahmen ergriffen wurden. Da Schulen je nach Größe und Schulform unterschiedlich organisiert sind, können die folgenden Hinweise nur Anregung und Hilfe sein und sollen eine Orientierung geben. An jeder Schule müssen die Datenschutzbeauftragten und IT-Sicherheitsbeauftragten in Absprache mit der Schulleitung prüfen, ob Besonderheiten vorliegen, die beim IT-Sicherheitskonzept zusätzlich berücksichtig werden müssen.	
Grundsätze	
Im Rahmen der Erfüllung ihres gesetzlichen Auftrages ist die einzelne Schule veranlasst, eine Fülle von Informationen und Daten über Schülerinnen und Schüler, Lehrkräfte, Eltern aber auch über die Unterrichtsorganisation vorzuhalten, zu speichern und zu verarbeiten. Dies geschieht nicht mehr nur in der herkömmlichen Form von Listen, Akten und Klassenbüchern, sondern in elektronischer Form. Die Rechtmäßigkeit der Erhebung und Verarbeitung solcher Daten ist vor allem durch das Schulgesetz NRW und die VO-DV I und VO-DV II geregelt. Grundsätzlich gilt, dass für jede Art von Erhebung und Verarbeitung personenbezogener Daten eine Rechtsverordnung oder eine Einwilligung der Betroffenen notwendig ist. Um das informationelle Selbstbestimmungsrecht der Beteiligten zu schützen, sind im Besonderen die Vorgaben des Datenschutzgesetz NRW (DSG-NRW) zu beachten.	

1. Aufklärungspflichten beim Erheben von Daten	
Schulen erhalten die ersten personenbezogenen Daten von Schülern und Eltern bei der Erstanmeldung der SuS an einer Schule oder z. B. über Schüler-Online bei den Berufskollegs. Soweit sie nicht aus den Systemen der Meldeämter übermittelt werden, erhebt die Schule die Daten bei Eltern und Schülern. Bei der Datenerhebung sind die Eltern bzw. die volljährigen Schüler auf die Tatsache hinzuweisen, dass diese Daten sowie weitere Daten, die im Rahmen des Schulbesuches entstehen und zur Dokumentation des Bildungsweges des Kindes notwendig sind, in der Schule gespeichert und verarbeitet werden (Aufklärungspflicht). Welche Daten dieses sind, regelt die „VO-DV I“.	
Darüber hinaus gehende Daten können die Schulen nur verarbeiten, wenn sie bei den Betroffenen und mit deren Zustimmung und Kenntnis erhoben wurden. Diese Einwilligung bedarf der Schriftform.	o.k. ☐

2. Maßnahmen zum Schutz personenbezogener Daten	
Es muss in der Schule sichergestellt sein, dass nur solche Personen Zugriff auf die in der Schule gespeicherten personenbezogenen Daten erhalten, bei denen für den Zugriff eine dienstliche Notwendigkeit besteht und die hierzu auch eine Befugnis haben. Dies gilt für Daten die in konventionellen Akten gehalten werden gleichermaßen wie für Zugriffe auf Daten in einem IT-Verfahren, zum Beispiel Schild-NRW. Dies bedeutet, dass Lehrkräfte grundsätzlich eine Zugangsberechtigung nur zu Daten der Schüler besitzen die sie unterrichten, nicht aber zu allen Schülern der Schule.	o.k. ☐
3. Zuständigkeiten	
Der Schulleiter ist gegenüber möglichen Betroffenen, dafür verantwortlich, dass allen datenschutzrechtlichen Vorschriften Vorgaben und Notwendigkeiten Rechnung getragen wird. Diese Vorschriften verlangen vor allem folgende Maßnahmen:	
• *Wenn gewünscht; die Bestellung eines schulischen Datenschutzbeauftragten in jeder Schule.(Optional)*	o.k. ☐
• Vorabkontrolle durch den behördlichen Datenschutzbeauftragten für den Kreis.	o.k. ☐
• Erstellung und Fortführung eines Verfahrensverzeichnisses, das beim behördlichen Datenschutzbeauftragten vorliegt und eingesehen werden kann.	o.k. ☐
• Erstellung, Fortführung und Umsetzung eines schriftlichen IT-Sicherheitskonzeptes.	o.k. ☐
• Abstimmung notwendiger Maßnahmen im Rahmen der äußeren Schulverwaltung mit dem Schulträger.	o.k. ☐

4. Technische und Organisatorische Maßnahmen	
4.1 Sicherstellung ausreichender Qualifikation.	
Das Personal, das für den Betrieb und die Wartung der IT in den Schulen zuständig ist, muss die ihm zu übertragenden Aufgaben fachkundig erfüllen können. Beauftragt der Schulträger eigenes oder externes Personal, so trägt er unmittelbar die Verantwortung für die fachliche Qualifizierung des IT Personals.	o.k. ☐
4.2 Räumliche Sicherung der IT-Anlagen	
Räume mit Netzstrukturen und IT-Systemen, die den Zugang auf das Verwaltungsnetz der Schulen bzw. auf das kommunale Schulträgernetz bereitstellen, unterliegen besonderen Schutzmaßnahmen, da die entsprechenden Gebäude der Öffentlichkeit während der regulären Dienstzeiten und gegebenenfalls auch zu bestimmten Anlässen auch an Wochenenden (z.B. Schulfeste oder Schule als Wahllokal) oder an Wochentagen nach der regulären Hauptarbeitszeit (z.B. Elternabende, Infoveranstaltungen etc.) zugänglich sind. Es müssen Maßnahmen und Regelungen getroffen werden, um den unberechtigten Zutritt zu schutzbedürftigen Räumen zu verhindern.	o.k. ☐
4.2.1 Zutrittskontrolle	
• Räume, in denen PCs oder Netzwerkkomponenten des Verwaltungsnetzes stehen, sollten mit einem geeigneten Schutz gegen unbefugten Zutritt und Einbruch etc. versehen sein. Ggf. ist dieser vom Schulträger einzufordern. Der Zutritt zu Räumen mit Netzstrukturen und IT-Systemen ist ausschließlich berechtigten Personen (Schulleitung, Lehrer, Verwaltungsangestellte, ggf. Netzwerkadministrator) gestattet.	o.k. ☐
• Die Räume müssen sicher verschließbar sein,	o.k. ☐
• Der Kreis der zutrittsberechtigten Personen muss genau festgelegt werden (z.B. durch dokumentierte Schlüsselverwaltung) und	o.k. ☐
• Die Kenntnisnahme der entsprechenden Regelungen durch die berechtigten Personen muss dokumentiert werden.	o.k. ☐
• Anderen Personen ist der Zutritt allenfalls in Begleitung oder Anwesenheit berechtigter Personen erlaubt.	o.k. ☐

Zu: 4.2.1 Zutrittskontrolle

• Für Personenkreise, die außerhalb der regulären Öffnungszeiten die Räume betreten müssen (z.B. Reinigungspersonal o.Ä.) können evtl. in Absprache mit dem Schulträger Sondervereinbarung getroffen werden.	o.k. ☐
• Bei nicht besetzten Räumen, in denen Client-Systeme bzw. Netzinfrastruktur stehen, sind Fenster und Türen verschlossen zu halten. Schlüssel zu diesen Räumen sind nur an berechtigte Personen (kontrolliert bzw. dokumentiert) auszugeben und dürfen nicht an andere Personen weitergegeben werden (Zugangs- und Zutrittsschutz).	o.k. ☐
4.3 Benutzer- und Zugriffskontrolle	
• Für ein gesichertes Login an einem IT-System ist die entsprechende Authentifizierung, bestehend aus dem Benutzernamen und einem geheim zu haltendem Passwort notwendig. Regelungen zur Wahl eines sicheren Passworts sollten sich an der „BSI Maßnahme M2.11 Regelung des Passwortgebrauchs“ orientieren (Zugangs- und Zugriffsschutz). Das Passwort ist personenbezogen zu halten und in angemessenen Zeiträumen zu wechseln.	o.k. ☐
• Passwörter sollen mindestens acht Zeichen umfassen und möglichst eine komplexe Zusammensetzung aus Buchstaben (groß/klein), Sonderzeichen und Ziffern aufweisen. Passwörter dürfen in keinem Fall zugänglich notiert oder an andere Personen weitergegeben werden. Für Notfall-Passwörter gilt die Ausnahme, dass diese in einem Passwort-Safe hinterlegt werden dürfen.	o.k. ☐

5. Verwaltungsnetz und Verwaltungsrechner	
Bei den kommenden Ausführungen wird vom (Schul-)Verwaltungsnetz und von Verwaltungsrechnern (ADV-Anlagen) gesprochen. Verwaltungsrechner sind alle Computersysteme, die ausschließlich für Verwaltungszwecke zu nutzen sind. Eine gleichzeitige Nutzung zur Unterrichtsvorbereitung oder Ähnlichem ist nicht gestattet. Verwaltungsrechner sind entweder Stand-Alone-Geräte, die mit keinem anderen Rechner verbunden sind, sie können Geräte in einem lokalen Schulverwaltungsnetz sein und sie können darüber hinaus an das Schulverwaltungsnetz des Schulministeriums angebunden sein. In keinem Fall dürfen sie über einen ungeschützten Internetzugang verfügen.	
Für Rechner im Verwaltungsbereich gilt: • Rechner, Datenträger und aktive Komponenten können nicht aus dem Unterrichtsbereich in den Verwaltungsbereich oder umgekehrt aus dem Verwaltungsbereich in den Unterrichtsbereich übernommen werden, ohne dass vorher vorhandene Software und Daten sicher gelöscht werden. Vorgehensweisen und Methoden werden im BSI Maßnahmenkatalog „M 2.167 Sicheres Löschen von Datenträgern“ beschrieben. Über das Löschen der Daten und Datenträger ist ein Vermerk zu den Akten zu nehmen.	o.k. ☐
• Techniker und für IT Software und Hardware verantwortliche Lehrkräfte wurden entsprechend belehrt.	o.k. ☐
• Entsprechend der Art des Einsatzes ist auf Schulverwaltungsrechnern auch nur solche Software einzusetzen, die zur Erfüllung dieser Aufgaben dient. Die Installation von nicht genehmigter Software (z.B. durch Downloads vom Internet oder von anderen Quellen) auf den Client-Rechnern ist nicht erlaubt und sollte nach Möglichkeit technisch unterbunden werden (Schutz vor unbeabsichtigter Installation von Schadsoftware und störende bzw. beeinträchtigende Wechselwirkungen mit benötigter Software). Auf Schulverwaltungsrechnern ist die Verträglichkeit der Software untereinander auf den Rechnern und insbesondere die aufgabengebundene Nutzung des PCs sicher zu stellen.	o.k. ☐

Zu: 5. Verwaltungsnetz und Verwaltungsrechner

• Befinden sich die Client-Systeme der Verwaltung im Verwaltungsnetz in Räumen mit Publikumsverkehr (z.B. Sekretariat oder dergleichen) ist durch eine geeignete Aufstellung der Client-Systeme (einschließlich Tastatur, Bildschirm, Drucker, Scanner und dergleichen) der Zugriff von Unbefugten zum System und die Einsichtnahme von Daten zu verhindern. Bei Abwesenheit der Zugriffsberechtigten ist das Client-System entweder ganz auszuschalten oder zu sperren. In jedem Fall muss sich spätestens nach 10 Minuten „Ruhephase“ ein mit Passwortschutz ausgestatteter Bildschirmschoner aktivieren (Zugangs- und Zugriffsschutz).	o.k. ☐
• Die Konfiguration bzw. die vorhandenen Sicherheitseinstellungen der Client-Rechner dürfen durch die Benutzer nicht verändert werden. Dies sollte nach Möglichkeit technisch unterbunden werden. Dies betrifft Soft- und Hardware. Bei entsprechenden Fragestellungen oder Problemen ist der Schulleiter und ggf. der für die Schule zuständige Support zu kontaktieren (Zugangs- und Zugriffsschutz).	o.k. ☐

6. Hardware	
6.1 Schulische Netzwerke	
• In der Regel existieren in den Schulen Netzwerkverbindungen für Verwaltungszwecke (sog. Verwaltungsnetz) und für pädagogisch-didaktische Zwecke (sog. pädagogisches Netzwerk). Diese beiden Netzwerke sind physikalisch oder logisch strikt voneinander getrennt zu halten, da ihr Schutzbedarf jeweils unterschiedlich ist und verschiedene Zugriffsberechtigungen vorliegen können (Schutz vor unbefugtem Zugriff auf die Netzinfrastruktur, Systeme und dort verarbeitete Daten).	o.k. ☐
• Eine sichere logische Trennung der Netze. Die Sicherheitskonzepte zur logischen Trennung sollten die im IT-Grundschutzhandbuch des „BSI im Baustein 7.11 Router „und Switches“ vorgesehenen Maßnahmen berücksichtigen und müssen dem aktuellen Stand der Technik entsprechen.	o.k. ☐
• Auf den Einsatz von WLAN in der Schulverwaltung sollte aus Sicherheitsgründen verzichtet werden (Schutz vor unbefugtem Zugriff auf die Netzinfrastruktur, Systeme und dort verarbeitete Daten). In besonders begründeten Ausnahmefällen kann der Einsatz von WLAN auf Basis eines entsprechenden Sicherheitskonzeptes erfolgen.	o.k. ☐
• Zentrale Netzwerktechnik wie Router, Switches und Hubs soll in gesicherten, nicht öffentlich zugänglichen Räumen oder Schutzschränken untergebracht werden (s. auch Vorgaben für die IT-Infrastruktur; Zugangs- und Zutrittsschutz).	o.k. ☐
• Lehrkräfte sind nur für den „First-Level Support“ zuständig.	o.k. ☐
6.2 Nutzung privater IT-Geräte	
• Private IT-Geräte dürfen grundsätzlich nicht zur Erledigung schulischer Verwaltungsarbeit benutzt werden. • Eine Ausnahme bildet die Nutzung von Rechnern am häuslichen Arbeitsplatz der Lehrkräfte. Die Nutzung eines häuslichen Arbeitsplatzes muss von der Schulleitung genehmigt werden.	o.k. ☐

6.3 Mobile IT-Geräte	
• Sollte die Einbindung von „mobilen IT-Geräten“ notwendig sein, müssen diese ausschließlich dienstlich genutzt werden und dürfen in keiner Form anders als über das Schulverwaltungsnetz mit dem Internet verbunden werden.	o.k. ☐
6.4 Mobile Datenträger	
Werden personenbezogene Daten auf mobile Datenträger ausgelagert, so ist mit entsprechender Sorgfalt zu verfahren:	
• Der Datenträger mit personenbezogenen Daten ist zu registrieren.	o.k. ☐
• Soll der Datenträger auch außerhalb des Schulsekretariats bzw. der Büroräume der Schulleitung genutzt werden, so sind personenbezogene Daten zu verschlüsseln und ein gesicherter, überwachter Transport zu gewährleisten.	o.k. ☐
• Dienstlich gestellte Datenträger dürfen grundsätzlich nur für dienstliche Zwecke und zum Datentransport zwischen Verwaltungsrechnern verwendet werden.	o.k. ☐
• Werden die auf mobilen Datenträgern gespeicherten Daten nicht mehr benötigt, sind sie in das zentrale System zurückzuspielen und auf dem mobilen Datenträger sicher zu löschen (siehe BSI Grundschutz).	o.k. ☐

7. Schutz vor Schadprogrammen	
In den dezentralen Netzen liegt die Verantwortung für einen funktionsfähigen und stets aktuellen Schutz vor Schadprogrammen beim Schulleiter und Schulträger gleichermaßen.	
Zu den Aufgaben der Schulleitung gehören unter anderem:	
• die Sensibilisierung der Nutzer für vorhandene Gefahren durch Viren,	o.k. ☐
• die Information der Nutzer über Vorsichtsmaßnahmen und Verhaltensregeln zum Schutz vor Viren,	o.k. ☐
• dafür zu sorgen, dass geeignete Virenschutzmaßnahmen auf gefährdeten IT-Systemen implementiert werden,	o.k. ☐
• das Aufstellen von Verhaltensregeln für einen eingetretenen oder vermuteten Virenbefall, z.B. Benachrichtigung einer Hotline oder des IT-Supports, um eine Beseitigung der Virusinfektion zu veranlassen und sofortiges Einstellen der Arbeit am befallenen Client-Rechner.	o.k. ☐

8. Konventionelle und elektronische Datenspeicherung und Datensicherung	
8.1 Aufbewahrung von Schülerakten	
Die Schülerakten, Karteikarten mit personenbezogenen Angaben, entsprechende Listen etc. sind grundsätzlich nur in ausreichend sicheren Schränken zu verwahren (Stahlschrank mit Sicherheitsschloss o.Ä.). Bei größeren Schulsystemen empfiehlt es sich, die Akten stufen- oder zweigweise gegliedert in unterschiedlichen Schränken aufzubewahren, so dass dann, wenn ein Zugang notwendig wird, nie der gesamte Aktenbestand angeboten werden muss.	o.k. ☐
8.2 Elektronische Speicherung	
Werden über die Nutzung von Schulverwaltungsprogrammen (z.B. Schild NRW hinaus in der Schule elektronische Dokumente auf Verwaltungsrechnern gespeichert, so ist dafür – ggf. in Absprache mit dem Schulträger – ein entsprechendes Dateiablage-Konzept zu entwickeln. Handelt es sich um Dateien mit personenbezogenen Inhalten, muss der Zugang zu den entsprechenden Ablagesegmenten ausreichend geschützt werden, handelt es sich dabei auch um besonders schützenswerte Daten (z. B. Gesundheitsdaten), sind diese Daten zwingend verschlüsselt abzulegen.	o.k. ☐

8.3 Datensicherung	
• Zur Gewährleistung von Datenschutz und IT-Sicherheit gehört auch, dass die Verfügbarkeit der Daten gesichert ist. Dazu ist es notwendig, dass in Absprache mit dem Schulträger ein entsprechendes Datensicherungssystem eingerichtet ist. Die Datensicherung hat regelmäßig und in ausreichender Frequenz zu erfolgen (Tages-, Wochen- und Monatssicherung).	o.k. ☐
• Die Datenträger, auf denen diese Datensicherung erfolgt sind entsprechend der Sensibilität der jeweiligen Dateien geschützt aufzubewahren. Dies bedeutet nicht nur den Schutz vor unbefugten Zugriffen, sondern auch vor Beschädigung durch Feuer, Wasser oder Diebstahl. Daher sind sie nicht im gleichen Raum wie Rechner oder Server aufzubewahren, sondern in einem anderen entfernt liegendem Raum.	o.k. ☐
• Existiert an der Schule ein Client-Server-System, so sind die Daten grundsätzlich auf dem Server zu speichern. Die Daten auf dem Server sind zentral zu sichern und die Datenträger vorzugsweise in separaten Räumlichkeiten zu verwahren.	o.k. ☐
• Zusätzliche lokale Speicherung personenbezogener Daten auf den Clients hat zu unterbleiben.	o.k. ☐

9. Elektronischer Mailverkehr	
9.1 Allgemeine Grundsätze der Nutzung	
• Die dienstliche Mailadresse ist nur für dienstliche Zwecke zu nutzen. Im innerbehördlichen Schriftverkehr können Schreiben und sonstige Dokumente per E-Mail versandt werden, die nicht eine persönliche Unterschrift erfordern oder vertraulich zu behandelnde Daten enthalten • Der Versandt von E-Mail über das Internet mit personenbezogenen oder vertraulichen Angaben (z.B. Entwürfe für Prüfungsarbeiten) ist grundsätzlich ohne Verschlüsselung (BSI-Standard) nicht zulässig. Die Schulleitungen belehren hierzu gesondert die Lehrkräfte	o.k. ☐ o.k. ☐
9.2 Mail-Umleitung	
Eine Umleitung von Mails auf Postfächer im Internet birgt immer die Gefahr, dass Mails von nicht berechtigten Personen gelesen und auch verändert werden können. Daher gilt:	
• Eine automatisierte Umleitung darf Übrigen nur auf solche Postfächer eingerichtet werden, die sich im Schulnetz oder einem entsprechend abgesicherten Netz des Schulträgers befinden.	o.k. ☐
• Eine manuelle Umleitung auf Postfächer im Internet ist nur im Einzelfall zulässig und auch nur dann, wenn geprüft wurde, dass die Mail keine vertraulichen oder personenbezogenen Daten enthält.	o.k. ☐
• Es ist grundsätzlich zu beachten, dass bei umgeleiteten Mails und der Nutzung der „Antworten-Funktion“ als Absenderangabe nicht mehr die offizielle Schuladresse erscheint.	o.k. ☐
9.3 Geschützte Dokumente und Anlagen	
• Es ist notwendig, Dokumente, die man vor Veränderungen schützen will, im PDF-Format zu versenden. Dieses Format erfordert in der Regel auch weniger Speicherplatz.	o.k. ☐
• Versendet man mit einer E-Mail Dokumente als Anhang, so ist auf deren Größe zu achten, vor allem, wenn ein großer Adressatenkreis erreicht werden soll. Ausführbare Dateien (Endungen wie exe oder mdb) sollten nicht versandt oder empfangen werden.	o.k. ☐

Checkliste abgearbeitet:

Datum:

_____

Schulleitung

Datenschutzbeauftragter Schule