Sicherer Umgang mit dem privaten Endgerät

Leitfaden für Schulleitungen und Lehrkräfte

Mecklenburg Vorpommern
Ministerium für Bildung, Wissenschaft und Kultur

Einführung

Um Sie als Schulleiterinnen, Schulleiter, Lehrerinnen und Lehrer bei der täglichen Arbeit im Umgang mit Datenschutz und Datensicherheit zu unterstützen, hat das Bildungsministerium MV in Abstimmung mit dem Zweckverband eGo MV diesen Leitfaden entwickelt. Es handelt sich hierbei um keine Änderung oder Verschärfung geltender Regeln. Der Schwerpunkt liegt auf Hilfestellungen für den (freiwilligen) Einsatz privater Endgeräte an Schulen. Der Leitfaden enthält:

- allgemeine Hinweise zur freiwilligen Nutzung privater Endgeräte und Haftung,
- organisatorische und technische Umsetzungshinweise,
- eine Checkliste: Maßnahmen zur Prüfung der Umsetzung von Datenschutz und Datensicherheit,
  - ein Glossar,
  - eine Ausnahmeerlaubnis.

Ziel des Leitfadens ist es, Ihnen bei der Umsetzung der geltenden Anforderungen zu helfen, Empfehlungen zu geben, und Ihnen mit der Checkliste ein einfaches Werkzeug für ein Gespräch über die Nutzung privater Endgeräte zwischen Lehrkraft und Schulleitung zur Verfügung zu stellen. Zudem finden Sie im Anhang ein Glossar sowie den überarbeiteten Vordruck für die Ausnahmeerlaubnis (s. Anlage 1), den Sie an Ihrer Schule für die Abstimmung und Organisation privater Geräte nutzen können.

Die technischen und organisatorischen Maßnahmen zur sicheren Nutzung privater Endgeräte stellen Mindestanforderungen sowie weitere Empfehlungen aus Sicht der IT-Sicherheit und des Datenschutzes dar. Diese dienen nicht nur der sicheren dienstlichen Nutzung, sondern auch der Sicherheit Ihrer persönlichen Daten.

Die Erwartung ist nicht, dass von vornherein alle optionalen Empfehlungen umgesetzt werden – wichtig ist vielmehr, dass Sie sich des Themas annehmen und die Punkte schrittweise angehen.

Hinweis zur Information des ZV eGo MV im November 2020

Im November 2020 hat der Zweckverband eGo MV eine kurze Checkliste und ein Formular für die Ausnahmeerlaubnis zur Nutzung privater Endgeräte entwickelt und den Schulen, die den eGo mit Datenschutzaufgaben beauftragt haben, zur Verfügung gestellt.

Beide Dokumente des eGo MV sind weiterhin gültig und richtig. Lediglich die Abfrage der Seriennummer wurde mittlerweile abgeschwächt auf die letzten vier Ziffern. Sollten Sie die Ausnahmeerlaubnis in der Variante des eGo bereits in Verwendung haben, müssen Sie diese nicht nochmal beschließen. Vielleicht finden Sie trotzdem weitere nützliche Tipps in diesem Leitfaden.

Dieser Leitfaden enthält alle Punkte, die der eGo MV auch aufgegriffen hat, sowie zusätzliche Hinweise und Tipps.

Allgemeine Hinweise zur Nutzung privater Endgeräte

Private Endgeräte per Ausnahmeerlaubnis

Im Regelbetrieb sind private Endgeräte gem. § 7 der Schuldatenschutzverordnung M-V vom 23.04.2020 nur für solche dienstlichen Tätigkeiten zulässig, die ohne die Verarbeitung personenbezogener Daten auskommen (z. B. Unterrichtsvorbereitungen). Die Schulleitung als verantwortliche Stelle kann im Ausnahmefall (z. B. aufgrund einer Pandemie) die Erlaubnis erteilen, dass Lehrkräfte unter bestimmten Bedingungen ihre privaten Endgeräte auch für die Verarbeitung personenbezogener Daten von Schülerinnen und Schülern nutzen dürfen. Diese Ausnahme besteht aktuell und noch solange, bis die vollständige Rückkehr zum Präsenzunterricht erfolgt ist. Diese Bedingungen umfassen (und werden im Leitfaden erläutert):

- Kennwortschutz,
- aktuelles Betriebssystem,
- Virenschutz,
- Datenverschlüsselung,
- Transportverschlüsselung,
- WLAN-Passwort,
- Speicherort.

Zur Erfüllung dieser Bedingungen kann jede Lehrkraft die Lösung finden, die am besten zum genutzten Endgerät und den persönlichen Präferenzen passt.

Zwecks gemeinsamer Verbindlichkeit wird die Erlaubnis zur Nutzung des privaten Endgeräts beidseitig dokumentiert – hierfür finden Sie in Anlage 1 ein Formular. Die Schulleitung erlaubt die Nutzung und im Gegenzug verpflichtet sich die Lehrkraft, sich an die geltenden Regeln hierfür zu halten.

Haftung

Die Umsetzung der Regelungen und Anforderungen ist nicht immer einfach. Die Sorge, Fehler zu machen und hierfür im schlimmsten Fall sogar mit rechtlichen Konsequenzen rechnen zu müssen, ist verständlich. Eine schützende Lossagung für Lehrkräfte gibt es leider nicht, jedoch lässt sich die Sorge entschärfen und die Frage nach der Haftung einordnen:

Handelt eine Beamtin/ein Beamter bzw. eine Beschäftigte/ein Beschäftigter in Ausübung der dienstlichen Tätigkeit und es entsteht hierbei einem Dritten ein Schaden, haftet nach den Amtshaftungsgrundsätzen im Außenverhältnis zunächst der Staat bzw. die Körperschaft, in deren Dienst der Beamte bzw. der Beschäftigte steht. Dies ergibt sich aus § 839 BGB in Verbindung mit Art. 34 GG.

Erst im Anschluss wird ein Rückgriff im Innenverhältnis geprüft. Und hier gilt: Nur, wenn von Vorsatz oder grob fahrlässigen Verhaltens auszugehen ist, könnte ggf. ein Regressanspruch in Betracht kommen. Dabei gelten die einschlägigen Vorschriften des Beamtenstatusgesetzes in Verbindung mit dem Landesbeamtengesetz bzw. bei Beschäftigten die Vorschriften des Tarifvertrages für den öffentlichen Dienst der Länder (TV-L). Die rechtlichen Grundlagen hierfür finden sich in § 839 BGB i.V.m. Art. 34 GG und § 52 LBG i.V.M. § 48 BeamtStG bzw. § 3 Abs. 7 TV-L für Tarifbeschäftigte.

Datenschutzfragen

Bei weiterführenden Fragen zum Datenschutz können Sie sich an den Zwecksverband eGo MV wenden, den Sie unter der Telefonnummer 0385 773347-51 bzw. der E-Mail datenschutz@ego-mv.de erreichen.

Technische und organisatorische Umsetzungshinweise zur sicheren Nutzung von Endgeräten

Die nachfolgenden Sicherheitshinweise basieren auf Umsetzungsempfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der Allianz für Cyber-Sicherheit.

Die wesentliche Strategie, die dabei genutzt wird, ist das so genannte Erforderlichkeitsprinzip. Im Wesentlichen bedeutet dies, dass Sie bei Ihrer Arbeit stets restriktiv bewerten, ob Sie eine Information wirklich wissen bzw. weitergeben müssen. Nachfolgend finden Sie auf Basis dieser Strategie technische und organisatorische Maßnahmen, die für Ihren (Arbeits-)Alltag relevant sind. Weiterführende Umsetzungshinweise erhalten Sie auf der Webseite des BSI (Links zu einzelnen Themen finden Sie in Anlage 3 dieses Dokuments). Zudem steht Ihnen der ZV eGo MV als zentraler Ansprechpartner für den Datenschutz an öffentlichen Schulen in Mecklenburg-Vorpommern zur Verfügung.

Technische Maßnahmen

T1: Führen Sie regelmäßig Aktualisierungen durch

Veraltete Software weist oft kritische Sicherheitslücken auf. Viele dieser Lücken werden öffentlich kommuniziert, um mögliche Softwareupdates bereitzustellen. Daher ist es wichtig, das Betriebssystem sowie jegliche andere Software auf einem möglichst aktuellen Stand zu halten. Dies kann heutzutage über die Nutzung der Funktion zur automatischen Aktualisierung komfortabel umgesetzt werden. Nach dem eingangs erwähnten Erforderlichkeitsprinzip empfiehlt es sich, Programme die längere Zeit nicht in Anspruch genommen wurden, zu deinstallieren. Denn die Angriffsfläche wird kleiner, desto weniger Programme auf Ihrem System installiert sind.

T2: Verwenden Sie einen aktuellen Virenschutz und Firewall

Zum Schutz vor externen Angriffen ist eine Firewall essenziell. Eine Firewall ist ein Sicherungssystem, das Computer vor unerwünschten Netzwerkzugriffen schützt. Sollte doch einmal eine Schadsoftware auf Ihren Rechner platziert worden sein, greift im besten Fall der Virenschutz. Beide Komponenten (Virenschutz und Firewall) sind

in den gängigen Betriebssystemen integriert. Prüfen Sie, ob diese beiden Komponenten aktiviert sind. Alternativ können Sie auch den Virenschutz und die Firewall eines anderen Anbieters einsetzen. Aber denken Sie daran, die erste und wichtigste Maßnahme ist Ihre eigene Aufmerksamkeit.

T3: Verwenden Sie verschiedene Benutzerkonten/Passwörter für verschiedene Einsatzzwecke

Schadprogramme erhalten die gleichen Rechte wie die angemeldete Nutzerin/der angemeldete Nutzer, der sie unabsichtlich installiert bzw. ausgeführt hat. Daher ist es wichtig, dass im täglichen Betrieb ein Benutzerkonto verwendet wird, was keinem Administrator entspricht. Am besten richten Sie sich ein eigenes Benutzerprofil für dienstliche Zwecke ein. Werden Administratorrechte benötigt, wird explizit nach dem Passwort gefragt, so dass Sie mitbekommen, ob ein Programm unerlaubte Funktionen aufruft. Dieser Rat gilt auch für Passwörter. Verwenden Sie bitte unterschiedliche Passwörter für unterschiedliche Dienste (E-Mail, Lernmanagement-Software, Online-Banking, usw.). Hierfür eignen sich auch Passwortprogramme.

T4: Achten Sie darauf, dass Sie einen aktuellen Webbrowser verwenden

Bei der Verwendung von Webbrowsern ist darauf zu achten, dass diese noch vom Hersteller unterstützt werden. Somit ist garantiert, dass wesentliche Sicherheitsupdates noch bereitgestellt werden können. Da auch Werbung auf schadhafte bzw. unerwünschte Internetseiten/Inhalte führen kann, sollten Sie nach Möglichkeit einen sogenannten Werbeblocker (engl. ad blocker) verwenden. Des Weiteren überprüfen Sie die Einstellungsmöglichkeiten Ihres Browsers, um unerwünschte Datenabflüsse zu vermeiden (z. B. „privater Modus“, „Verlauf löschen“, „Cookies nicht für Drittanbieter zulassen“). Sind Sie sich bei einem Link zu einer bekannten Seite nicht sicher, dann geben Sie die Adresse per Hand in die Adressleiste Ihres Browsers ein und verzichten auf die Nutzung des Links.

T5: Setzen Sie auf eine starke Verschlüsselung Ihrer sensiblen und personenbezogenen Daten

Mittels einer Verschlüsselung können Daten bei der Übertragung und/oder Speicherung vor dem Zugriff durch unberechtigte Dritte geschützt werden. Für das Surfen mit einem Browser nutzen Sie bitte nur verschlüsselte Verbindungen wie das https-Protokoll. Sie erkennen in Ihrem Webbrowser, dass eine gültige Verschlüsselung vorliegt an einem geschlossenen Schloss-Symbol neben der eigentlichen Internetadresse. Bei der Übertragung von sensiblen und personenbezogenen Daten nutzen Sie bitte die Möglichkeit der Verschlüsselung von E-Mails und deren Anhängen (z. B. mit dem Programm 7zip mit zusätzlichem Passwort).

Vorzugsweise sollten Sie ein kabelgebundenes Netzwerk nutzen, alternativ ein ausreichend gesichertes WLAN. Daher ist darauf zu achten, dass dieses nach dem Stand der Technik (mind. WPA2) verschlüsselt und mit einem ausreichend sicheren Passwort (mind. 20 Zeichen) geschützt ist. Auch die Daten auf dem eigentlichen Endgerät sollten durch eine dem Schutzbedarf der Daten entsprechende Verschlüsselung geschützt sein. Hierfür bietet sich die Möglichkeit der Festplatten-, Ordner-, o. USB-Stick-Verschlüsselung an. In gängigen Betriebssystemen gibt es bereits integrierte Lösungen (MacOS: FileVault, Windows: EFS). Auch mobile Endgeräte (IOS: standardmäßig aktiv, Android: meist über Einstellungen aktivierbar) bieten diese Möglichkeiten an.

T6: Nutzen Sie nur schuleigene Cloud-Speicher-Dienste

Nutzen Sie keine privaten Cloudspeicher von Dritten (z. B. Dropbox) für die Speicherung von dienstlichen personenbezogenen Daten.

Organisatorische Maßnahmen

O1: Gehen Sie sorgsam mit sensiblen und personenbezogenen Daten um

Eines der wichtigsten Güter, die wir derzeit haben, sind Informationen. Diese können einen beachtlichen Wert besitzen und sind daher oftmals Ziel von sogenannten Hackerangriffen oder Social Engineering. Insbesondere bei personenbezogenen Daten kann dies neben einem materiellen Schaden auch einen immensen immateriellen Schaden zu Folge haben, wenn diese publik werden. Daher ist es umso wichtiger, dass Unbefugte keinen Zugriff/Einblick auf die Informationen erhalten, wenn sie erstellt, transportiert oder entsorgt werden. Es gilt dabei den ganzen Lebenszyklus einer Information zu schützen.

Vermeiden Sie daher öffentliche WLAN-Zugänge und nutzen Sie Ihr gesichertes Heimnetzwerk. Eventuell steht Ihnen ein VPN-Netzwerk zur Verfügung, dass Sie nutzen können. Sollten Unterlagen nicht mehr benötigt werden, entsorgen Sie diese bitte fachgerecht (z. B. in Ihrer Dienststelle)

O2: Schaffen Sie sich nach Möglichkeit einen Arbeitsraum

Es ist empfehlenswert, einen adäquaten Raum für Ihre Arbeit zu nutzen, der über einen entsprechenden Zutrittsschutz und Sichtschutz verfügt. Auch bei kurzer Abwesenheit sind die technischen Geräte zu sperren (z. B. Bildschirmsperre bei Windowsgeräten über Windowstaste + kleines „L“ oder Strg+Alt+Entf/Ende). Bei längerer Abwesenheit und Dienstschluss: Melden Sie sich von Fachanwendungen ab und fahren Sie Ihre Endgeräte herunter. Außerdem sind ebenso die Arbeitsmittel, Unterlagen, Akten usw. zugangsgesichert und verschlossen zu verwahren (z. B. Schrank, Raum). Sollten entsprechende Verschlussmöglichkeiten nicht vorhanden sein, sind die Geräte anderweitig vor dem Zugriff durch Dritte (insbesondere Familienmitglieder) geschützt zu lagern.

O3: Sicherer Umgang mit E-Mails

Die meisten erfolgreichen Angriffe durch Dritte basieren auf sogenannten Fake- oder Phishing-E-Mails. Zum Teil werden bekannte alte Konversationen aufgegriffen, um Ihnen ein Gefühl der Vertrautheit zu vermitteln und um Sie dazu zu verleiten, schadhafte Anhänge oder Links zu öffnen. Fragen Sie sich immer: „Ist der Absender bekannt?“, „Ist der Betreff sinnvoll?“ und „Erwarte ich einen Anhang von diesem Absender?“ Hierdurch sind Sie in der Lage, einzuschätzen, ob die E-Mail vertrauenswürdig ist. Haben Sie Zweifel an der Authentizität der E-Mail, kontaktieren Sie den vermeintlichen Absender direkt z. B. durch einen Anruf.

O4: Nutzen Sie vertrauenswürdige Quellen für jegliche Downloads (Software, Medien, Updates)

Sollten Sie Daten aus dem Internet benötigen, laden Sie diese bitte direkt vom Hersteller herunter. Laden Sie die Daten von anderen Quellen, könnte Schadsoftware (z. B. Ad Malware) in den Daten versteckt sein. Es empfiehlt sich immer, die heruntergeladenen Daten mittels einer aktuellen Anti-Viren-Software zu prüfen.

O5: Vergessen Sie das Backup nicht

Erstellen Sie regelmäßig Backups von Ihren wichtigen Daten. Sollte ein Angriff auf Ihr Endgerät erfolgreich sein, so haben Sie die Möglichkeit, Ihre Daten wiederherzustellen. In der Regel werden durch Angriffe Ihre Daten auf Ihrem Gerät verschlüsselt. Gehen Sie nicht auf etwaige Erpressungsversuche ein, es gibt keine Garantien, dass die Angreifer Ihre Daten wieder entschlüsseln werden. Informieren Sie umgehend Ihre Schulleitung.

O6: Meldepflicht für Diebstahl oder Verlust von Endgeräten oder Datenträgern

Jede Sekunde zählt, wenn sensible oder personenbezogene Daten betroffen sind. Melden Sie daher unverzüglich den Verlust oder Diebstahl eines Endgerätes oder Datenträgers bei Ihrer Schulleitung und Ihrem bestellten Datenschutzbeauftragten.

Checkliste: Maßnahmen zur Prüfung der Umsetzung von Datenschutz und Datensicherheit

Grundlegende Bedingungen

Prüfen Sie zunächst, ob die folgenden drei grundlegenden Bedingungen auf Sie zutreffen – denn nur dann kommt die Ausnahme-Erlaubnis für Sie in Frage:

- Sie haben nicht die Möglichkeit, die Verarbeitung personenbezogener Daten mittels dienstlicher Endgeräte durchzuführen.
- Sie verarbeiten lediglich personenbezogene Daten der Schülerinnen und Schüler, die Sie selbst unterrichten nach Anlage 2 der SchulDSVO M-V sowie in einer Lernsoftware nach §5a Abs. 7 SchulDSVO M-V.
- Sie vermeiden öffentliche WLAN-Zugänge mit Ihrem Endgerät und verfügen zum Arbeiten über einen eigenen Internet-Zugang.

Checkliste

Die Checkliste mit den konkreten Vorgaben (verpflichtend) sowie weitergehenden Empfehlungen (optional) dient als Hilfestellung und gibt Hinweise, welche Einstellungen nach dem derzeitigen Stand der Technik umgesetzt werden müssen. Um Ihnen die Orientierung zu vereinfachen, wurde die Spalte „Bezug" eingeführt, sodass Sie gegebenenfalls in den Hinweisen des vorherigen Kapitels nachlesen können.

Nr.	Technische und organisatorische Maßnahmen Vorgaben nach §7 Abs. 4 SchulDSVO M-V	Bezug	Check
1	Das verwendete **Betriebssystem** aktualisiert sich automatisch.	T1	☐
2	Es ist eine aktive **Firewall** und aktive Antivirensoftware installiert, die sich automatisch aktualisiert.	T2	☐
3	Das Endgerät ist gegen unbefugten Zugriff durch Dritte mittels **Kennwort und/oder biometrischem Erkennungsverfahren** zu sichern. Stellen Sie ein, dass der Computer sich nach einigen Minuten Untätigkeit automatisch wieder sperrt. Wird ein Passwort eingesetzt, sollte es mindestens 10 Zeichen lang sein und drei von vier der folgenden Kriterien erfüllen: Großbuchstabe, Kleinbuchstabe, Zahl, Sonderzeichen.	T3	☐
4	Dienstliche Datenbestände auf dem Endgerät als auch auf mobilen Datenträgern sind **verschlüsselt**. Nutzen Sie z. B. EFS für Windows oder FileVault für macOS.	T3	☐
5	Beim elektronischen Versand von Informationen und Dateien ist, wenn verfügbar, eine **Transportverschlüsselung** zu nutzen und gegebenenfalls eine Dateiverschlüsselung (z. B. 7-zip, Office Verschlüsselung). Idealer Weise nutzen Sie nach Möglichkeit das LMS zum Austausch von Dateien, da hier keine zusätzliche Verschlüsselung mehr nötig ist.	T4	☐
6	Das private **WLAN** ist mindestens mit WPA2 verschlüsselt und der WLAN-Schlüssel ist mindestens 20 Zeichen lang.	T5	☐
7	Sie nutzen **keine privaten Cloudspeicher von Dritten** (z. B. Dropbox) für die Speicherung von personenbezogenen Daten. Sie wurden auf die Vermeidung von privat genutzten Clouddiensten hingewiesen. Verwenden Sie soweit möglich die Lernmanagementsoftware Ihrer Schule.	T6	☐

Weitergehende Empfehlungen und Tipps (optional)			
Nr.		**Bezug**	**Check**
1	Sie nutzen Ihr Endgerät zur Arbeit in einem eigenen Arbeitszimmer mit Sichtschutz oder haben die Möglichkeit, dienstliche Unterlagen sicher zu verschließen.	O2	☐
2	Sollte das Gerät nicht ausschließlich dienstlich genutzt werden, richten Sie ein zusätzliches dienstliches Konto ein.	O2	☐
3	Sie haben einen dienstlichen Ansprechpartner, an den Sie sich wenden können, wenn Sie sich bei E-Mails oder anderen Links unsicher sind, ob diese schadhaft sein könnten.	O3	☐
4	Software, mit der Sie personenbezogene Daten verarbeiten, stammt aus vertrauenswürdigen Quellen (z. B. direkt vom Softwarehersteller) und wurden von der Schulleitung zur Kenntnis genommen.	T3	☐
5	Sie sichern regelmäßig Ihre dienstlichen Daten und die Sicherung ist vor einem externen Zugriff geschützt (sichere Aufbewahrung des Sicherungsmediums wie eine verschlüsselte externe Festplatte).	O4	☐
6	Sie kennen die Person, an die Sie einen Diebstahl/Verlust Ihres Gerätes melden müssen. Der benannte Datenschutzbeauftragte sowie die Schulleitung sollten umgehend informiert werden.	O5	☐
7	Sie führen regelmäßig Updates der installierten Software auf Ihrem Endgerät durch.	T1	☐
8	Ihr Passwort für die Schuldienste ist ein anderes als Ihr Passwort für Ihr Endgerät.	T3	☐
9	Sie nutzen einen Passwortmanager um viele verschiedene Passwörter zu generieren und zu speichern. Sie müssen sich nur noch ein „starkes“ Passwort merken.	T3	☐
10	Sie nutzen einen aktuellen Browser.	T4	☐
11	Sie setzen einen Werbeblocker ein, um unerwünschte Werbung im Browser zu blockieren.	T4	☐
12	Ihr (WLAN)-Router hat nach dem Kauf ein neues Administrationspasswort durch Sie erhalten, welches sehr „stark“ ist. Empfohlen werden mindestens 10 Zeichen.	T5	☐

Anlage 1 – Ausnahme-Erlaubnis

für die Verarbeitung von personenbezogenen Daten durch Lehrkräfte und sonstiges Schulpersonal zu dienstlichen Zwecken auf privaten Datenverarbeitungsanlagen gemäß § 7 SchulDSVO-M-V.

1. Name und Anschrift der datenverarbeitenden Stelle

Name und Anschrift der Schule	
Name der Schulleiterin / des Schulleiters	
Name der Lehrkraft / sonstiges Schulpersonal	
Für die Nutzung vorgesehene(s) private(s) Endgerät(e)	
• genaue Bezeichnung	
• Seriennummer (die letzten 4 Ziffern sind ausreichend)	

2. Covid-19-Übergangserlaubnis

Aufgrund der aktuellen Krisensituation (Corona-Pandemie) und der damit einhergehenden Schwierigkeit einen ordnungsgemäßen Unterricht zu gewährleisten sowie in Ermangelung ausreichender schulischer Datenverarbeitungsanlagen, erteile ich die Erlaubnis zur Verarbeitung der oben genannten Daten zu dienstlichen Zwecken auf den unter 1. genannten privaten Endgeräten unter Einhaltung der Checkliste „Maßnahmen zur Prüfung der Umsetzung von Datenschutz und Datensicherheit".

Ich erteile des Weiteren die Erlaubnis, die aufgeführten mobilen privaten Endgeräte für die dienstliche Nutzung innerhalb der Schule mitzuführen. Eine Aufbewahrung der Geräte über Nacht in Gebäuden der Schule ist nicht zulässig. Die erteilte Erlaubnis gilt bis zum Ende des Ausnahmezustands oder bis zum Widerruf durch die Schulleitung. Sollte darüber hinaus keine Rückkehr zum vollständigen Präsenzunterricht möglich sein, so kann die Befristung entsprechend verlängert werden. Sobald der Lehrkraft ein Dienstgerät vorliegt, erlischt die Ausnahme-Erlaubnis automatisch.

Ort, Datum	Unterschrift der Schulleiterin / des Schulleiters

3. Verpflichtungserklärung

Name und Anschrift der Schule	
Name der Schulleiterin / des Schulleiters	
Name der Lehrkraft / sonstiges Schulpersonal	

Ich verpflichte mich, ausschließlich die in der Ausnahme-Erlaubnis genannten personenbezogenen Datensätze auf meinen privaten Endgeräten und die Daten auch nur für dienstliche Zwecke zu verarbeiten. Des Weiteren verpflichte ich mich, die technischen und organisatorischen Maßnahmen gemäß der Checkliste „Maßnahmen zur Prüfung der Umsetzung von Datenschutz und Datensicherheit“ umzusetzen und einzuhalten.

Sofern sich zuvor gemachte Angaben (insbesondere im Fall eines Gerätewechsels) ändern, informiere ich die Schulleitung umgehend darüber, dass die vorliegenden Unterlagen angepasst werden können. Ich wurde darüber in Kenntnis gesetzt, dass ich verpflichtet bin, der Schulleitung alle Auskünfte zu erteilen, die für die datenschutzrechtliche Verantwortung erforderlich sind. Ich verpflichte mich, Datenmissbrauch oder Datenverlust der bei mir verarbeiteten Daten umgehend der Schulleitung zu melden.

Ich nehme zur Kenntnis, dass die Schulleitung ein Recht darauf hat, die Einhaltung der technischen und organisatorischen Maßnahmen (nach der o.g. Checkliste) gemäß § 7 Absatz 5 der SchulDSVO M-V jährlich in den Räumlichkeiten der Schule zu kontrollieren. Ich bestätige diese Verpflichtung. Ein Exemplar dieser Verpflichtung habe ich erhalten.

Ort, Datum	Unterschrift der Schulleiterin / des Schulleiters

Anlage 2 – Verarbeitung von Datensätzen

Gemäß § 70 Schulgesetz M-V (SchulG M-V) in Verbindung mit § 7 Abs. 1 und Abs. 3 S. 2 Schuldatenschutzverordnung M-V (SchulDSVO M-V) und des Informationsschreibens des Bildungsministeriums zum Inkrafttreten der Schuldatenschutzverordnung vom 30.04.2020 sowie vom 04.11.2020 dürfen die folgenden erforderlichen Datensätze aus Anlage 2 zur SchulDSVO M-V sowie ausschließlich in einer Lernmanagementsoftware Datensätze gemäß § 5 a Abs. 7 SchulDSVO M-V, ausnahmsweise auf privaten Datenverarbeitungsgeräten verarbeitet werden (Stand: April 2020):

Anlage 2 SchulDSVO M-V

1. Name (einschließlich Geburtsname),
2. Vorname,
3. Geschlecht,
4. Geburtsdatum,
5. Klasse/Jahrgangsstufe, Kurs,
6. Schülernummer/Gesamtschülerverzeichnis,
7. Bildungsgang, Ausbildungsrichtung/Ausbildungsberuf, gegebenenfalls Schwerpunkt,
8. Fächer, in denen die Lehrkraft Schülerinnen und Schüler unterrichtet,
9. Ergebnisse und Teilergebnisse schriftlicher, mündlicher und praktischer Leistungsüberprüfungen, in den von der Lehrkraft erteilten Fächern sowie Art und Datum der Leistungserhebung beziehungsweise Bewertung und
10. Zeiten des Fernbleibens vom Unterricht in den Fächern, in denen die Lehrkraft die Schülerinnen und Schüler unterrichtet.

Die Schulleitung, deren Stellvertretung und gegebenenfalls weitere mit Leitungsaufgaben betraute Lehrkräfte dürfen darüber hinaus die folgenden Schülerdaten verarbeiten:

1. Halbjahresnoten in allen Fächern der betreffenden Schülerinnen und Schüler,
2. alle zeugnisrelevanten Leistungsangaben und
3. zeugnisübliche Bemerkungen.

§ 5 a Abs. 7 SchulDSVO M-V

In einer Lernsoftware dürfen folgende Kategorien von personenbezogenen Daten verarbeitet werden:

1. Kontaktinformationen (Name, Benutzername),
2. Kommunikation (Nachrichten zwischen Benutzern, Diskussionen, Kommentare zu Beiträgen, Benachrichtigungen),
3. Kursmaterialien,
4. Bewertungen (keine Benotung),
5. Kalendereinträge und Ereignisdaten,

Dokumente, Präsentationen, Videos, Bilder, Hausaufgaben, Aufgaben, Nachrichten.

Anlage 3 – Glossar / Linksammlung

Glossar	
Ad-Blocker	Werbeblocker – ein Programm, welches dafür sorgt, dass auf Webseiten enthaltene Werbung dem Betrachter nicht dargestellt wird. https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungBrowser/Adblocker_tracking/adblocker_tracking_node.html
Ad-Malware	Ad-Aware-Software, die eine Internet-Verbindung ohne explizite Zustimmung des Anwenders nutzt. Häufig werden persönliche Teil-Informationen ohne Wissen des PC-Besitzers an die Hersteller installierter Programme übermittelt, die in der Summe ein sehr genaues Profil Ihres Surf-Verhaltens ergeben. https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/Schadprogramme/schadprogramme_node.html
Backups	Eine Kopie, die man als Sicherung von einer Datei herstellt. https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Datensicherung/datensicherung_node.html
Benutzerkonto	Zugangsberechtigung zu einem zugangsbeschränkten IT-System, durch welche das System den Benutzer identifiziert. https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Benutzerkonten/benutzerkontennetzwerk_node.html
Browser	Software zur grafischen Darstellung des Internets. https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungBrowser/derbrowser_node.html
BSI	Bundesamt für Sicherheit in der Informationstechnik (BSI) mit der Aufgabe der Untersuchung von Sicherheitsrisiken bei der Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen.
Cloudspeicher	Ein Dienst, mit dem Daten gespeichert werden können, indem sie über das Internet oder ein anderes Netzwerk an ein standortexternes System übertragen werden, das von einem Dritten verwaltet wird. https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/CloudComputing/GefahrenRisiken/gefahrenrisiken_node.html

EFS	Encrypting File System (EFS) kennzeichnet ein System der Dateiverschlüsselung von Rechnern mit dem Betriebssystemen Windows 8 und Windows 10.
ZV eGo M-V	Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern (eGo-MV).
FileVault	Eine Funktion von Mac OS X/OS X/macOS zum Verschlüsseln von persönlichen Daten. https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Datenverschluesselung/Betriebssysteme/betriebssysteme_node.html
Firewall	Sicherungssystem, welches ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt. https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Schutzprogramme/schutzprogramme_node.html
https-Protokoll	Zustandsloses Protokoll zur Übertragung von Daten auf der Anwendungsschicht über ein Rechnernetz.
Passwort Manager	https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Umgang/umgang_node.html https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Passwort_Manager/Passwort_Manager_node.html https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Umgang/umgang_node.html
Phishing-E-Mails	Versuche, sich über gefälschte E-Mails als vertrauenswürdiger Kommunikationspartner in einer elektronischen Kommunikation auszugeben. https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/phishing_node.html
Signatur	Textabschnitt mit Angaben zum Absender
Updates	Eine neue und verbesserte Version eines Programms. https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/UpdatePatchManagement/updatePatchManagement_node.html
Verschlüsselung von Daten	https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Verschluesselung_node.html

Verschlüsselung von E-Mails	https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Verschluesseltkommunizieren/verschluesselt_kommunizieren_node.html
VPN	Virtuelles, privates Netzwerk: Darunter ist ein in sich geschlossenes Kommunikationsnetz zu verstehen. Es ist virtuell in dem Sinn, dass es keine eigene physische Verbindung aufweist, sondern ein bestehendes Kommunikationsnetz als Transportmedium verwendet. Es verbindet Teilnehmer des bestehenden Kommunikationsnetzes mit einem anderen Netz.
7zip	https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/EMail_Verschluesselung/In_der_Praxis/EMails_verschluesseln_in_der_Praxis_node.html
WLAN	Wireless Local Area Network: ein lokales Funknetz zur Datenübertragung. https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungWLAN-LAN/EinrichtungLAN-WLAN_node.html

Impressum

Herausgeber:
Ministerium für Bildung, Wissenschaft und Kultur
Mecklenburg-Vorpommern
Werderstr. 124
19055 Schwerin

E-Mail: presse@bm.mv-regierung.de
Tel.: 0385 588-7003
Fax: 0385 588-7082

Internet: www.bm.regierung-mv.de
www.bildung-mv.de

Verantwortlich: Henning Lipski (V.i.S.d.P.)

Ansprechperson: Cornelia Zielke, Leiterin des Referats „Digitalisierung im Schulbereich“

Layout und Satz: Wolfgang Hoyer

Stand: Mai 2021

Bildnachweise: S.1 (Titelblatt): Pixabay/StockSnap, S. 6: Pixabay/fancycrave1, S. 10/11: AdobeStock/ronstik, S. 14: Colourbox/Pressmaster, S. 18: Pixabay/StartupStockPhotos

Dem Ministerium für Bildung, Wissenschaft und Kultur
Mecklenburg-Vorpommern folgen:

Twitter
@bildung_mv

Instagram
@bildungsministerium_mv

Facebook
@bildungsministerium.mv

YouTube
@Ministerium für Bildung, Wissenschaft & Kultur MV