mit Aktualisierung 2021

Datenschutz beim Einsatz digitaler Medien in der Grundschule

Eine Handreichung für Lehrerinnen und Lehrer in Baden-Württemberg mit rechtlichen Grundlagen, pädagogischen Hinweisen und Fallbeispielen

Robert Rymeš, Roland Walter, Ulrich Iberer

dileg-SL

Inhaltsverzeichnis

Das Wichtigste auf zwei Seiten

Der Einsatz digitaler Medien, insbesondere der von mobilen Endgeräten (z.B. Tablets), hat enorme Potenziale für das Lernen und Lehren in der Grundschule. Allerdings wirft er auch neue Fragen auf: In kreativen und innovativen Unterrichtsformen in denen Kinder z.B. die Kamera- und Mikrofonfunktion von Tablets einsetzen, werden verschiedene **personenbezogene Daten** erfasst und gespeichert. Dies sind alle jene Informationen, die sich bestimmten, eindeutigen Personen zuordnen lassen – also auch Video-, Foto- und Sprachaufnahmen. Die Verarbeitung dieser Daten ist an Schulen nach der europäischen **Datenschutz-Grundverordnung** im Grundsatz zunächst verboten. Sie wird erst durch die informierte Einwilligung der Betroffenen bzw. deren Sorgeberechtigten rechtlich zulässig.
Alle Akteure an einer Schule müssen dafür Sorge tragen, dass bei der **Verarbeitung von personenbezogenen Daten** den Betroffenen kein Schaden entsteht. Die letztliche Verantwortung trägt die Schulleitung. Sie muss für umfassende **technische und organisatorische Maßnahmen** sorgen, die beispielsweise verhindern, dass Unbefugte Zugang zu Daten erhalten. Bestimmte Maßnahmen muss auch jede einzelne Lehrkraft im Rahmen ihrer Lehrtätigkeiten und möglicher weiterer Zuständigkeitsbereiche durchführen.
Beabsichtigen Lehrkräfte digitale Medien im Unterricht einzusetzen, ist es wichtig vorab die zum Datenschutz erforderlichen Maßnahmen zu bestimmen. Folgende Leitfragen können dabei unterstützen:

1 Entstehen personenbezogene Daten beim Einsatz von digitalen Medien?

Sollen personenbezogene Daten von Schülerinnen und Schülern verarbeitet werden, muss zuerst eine Rechtsgrundlage in Form einer **informierten Einwilligung** der Sorgeberechtigten geschaffen werden. Im Rahmen dieses (schriftlichen) Einverständnisses müssen Eltern u.a. über den Zweck (z.B. Veröffentlichung auf der Schulhomepage) der Datenverarbeitung und ihre Rechte (z.B. Widerrufsrecht) aufgeklärt werden. Umfassende Einwilligungen können zu Anfang der Schulzeit eingeholt werden und bleiben – sofern kein Widerruf erfolgt – für die Dauer der Schulzugehörigkeit gültig. Um die elterliche Zustimmung zu gewinnen, sollte der Einsatz digitaler Medien im Unterricht und die damit zusammenhängenden datenschutzrechtlichen Aspekte persönlich besprochen und diskutiert werden (z.B. im Rahmen eines Elternabends).

2 Mit welchen Geräten werden die personenbezogenen Daten erstellt und zwischengespeichert?

Sofern nur **schuleigene Geräte** (z.B. Tablets, Digi-Cam) bei der Erhebung der Daten (z.B. Videographie eines Rollenspiels) zum Einsatz kommen, bleiben die zu treffenden Maßnahmen überschaubar, da die schuleigene IT-Infrastruktur in der Regel be-

reits datenschutzkonform konfiguriert ist. Jedoch sollte die Lehrkraft unbedingt darauf achten, dass Daten auf gemeinschaftlich genutzten Geräten gelöscht werden, bevor diese von anderen Personen weiterverwendet werden.
Wenn Lehrkräfte im Unterricht **private Geräte** (z.B. Smartphone, Tablet, Laptop) verwenden möchten, müssen sie sich vorher der Schulleitung gegenüber dazu verpflichten, verschiedene technische und organisatorische Maßnahmen umzusetzen. Dazu müssen Lehrkräfte einen **Antrag auf Nutzung privater Datenverarbeitungsgeräte für dienstliche Zwecke** bei der Schulleitung stellen und genehmigen lassen.

3 Wohin werden personenbezogene Daten übertragen bzw. wer bekommt Zugang zu den Daten?

Wenn die im Unterricht generierten personenbezogenen Daten die **Schul-IT-Infrastruktur** (Eingabegeräte, Netzwerk, Server) nicht verlassen, sind keine besonderen, zusätzlichen Maßnahmen notwendig. Falls die Lehrkraft diese Daten auf **private Geräte** (z.B. PC, externe Festplatte, USB-Stick) übertragen möchte, benötigt sie auch hierfür die Genehmigung der Schulleitung (s.o.) und muss umfassende Maßnahmen zur Geräte- und Datensicherheit (z.B. Zugriffssperren, Datenverschlüsselung) umsetzen. **Schülerdaten** auf privaten Lehrergeräten müssen spätestens nach dem Ende des jeweils nächsten Schuljahres **gelöscht** werden.
In manchen Fällen sollen personenbezogene Daten (z.B. Schülerarbeiten) einer bestimmten Gruppe von Personen aus der Schulsphäre vorgeführt oder weitergeleitet werden (z.B. Publikum einer Schulveranstaltung, Elternschaft einer Klasse). In Einzelfällen veröffentlichen Schulen auch Fotos, Videos, Schülernamen etc. auf ihrer Homepage oder in der Tagespresse. Bei jeder **Weitergabe, Vorführung** oder **Veröffentlichung** von personenbezogenen Daten muss eine informierte Einwilligung der Sorgeberechtigten der betroffenen Schülerinnen und Schüler vorliegen.
Die Verwendung von **externen Cloudspeichern** (z.B. *Dropbox*), **cloudbasierten Apps** (z.B. *doodle*) und **Web-Plattformen** (z.B. *YouTube*) ist im Zusammenhang mit personenbezogenen Daten von Schülerinnen und Schülern rechtlich mit großen Unwägbarkeiten verbunden und nur unter strengen Auflagen (z.B. EU-Sitz des Anbieters, EU-Standort der Server, Vertrag zur Auftragsdatenverarbeitung) möglich.

Bei jeder Form der Verarbeitung personenbezogener Daten sollten Schulen auch **pädagogische Schritte** initiieren, um Kinder für datenschutzrechtliche Aspekte zu sensibilisieren. Beispielsweise hat das *Landesmedienzentrum Baden-Württemberg* im Kontext der *Leitperspektive Medienbildung* des Bildungsplans 2016 zwei Unterrichtsmodule[1] für die Grundschule veröffentlicht, in denen zahlreiche Aspekte des Datenschutzes mit unterschiedlichen Methoden behandelt werden.

1 sesam.lmz-bw.de/mediathek?inp=token:datenprofis

Aktualisierung 2021

Überblick

Die technischen und rechtlichen Rahmenbedingungen im Bereich des Datenschutzes ändern sich rasant. Daher ist es notwendig, unserer Erstauflage vom September 2019 dieses kleine Update hinzuzufügen, in dem wir auf zwei wichtige Entwicklungen hinweisen wollen:

- Der Gesetzgeber (in Baden-Württemberg) hat das Schulgesetz dahingehend angepasst, dass Bild- und Tonaufnahmen unter bestimmten Bedingungen ohne Einwilligung der Eltern rechtmäßig sind. Das Gesetz reduziert für Lehrerinnen und Lehrer die formalen Anforderungen und stärkt gleichzeitig die Rechte der Betroffenen.

- Besonders sensibel beim Einsatz von Tablets sind Anforderungen rund um das Thema „Löschen“, v.a. wenn mehrere Schülerinnen und Schüler ein Gerät nutzen sollen (abwechselnd, als Leihgerät, o.a.). Neue technische Funktionen bei iPads der Firma Apple ermöglichen es jetzt in einer effizienteren Form, vor dem Wechsel bzw. der Neuausgabe von Geräten die zuvor generierten Daten automatisiert zu löschen („Gastmodus“).

Die übrigen Inhalte der bisherigen Handreichung bleiben unverändert und behalten bis auf die beiden in diesem Update erwähnten Änderungen ihre Gültigkeit. Wie auch in der Erstauflage gilt für dieses Update: Wir geben keine rechtlichen Garantien. Das Feld des Datenschutzes ist dynamisch. Neue Gesetze, Verordnungen und Urteile schaffen veränderte Anforderungen und Verantwortungen. Sie eröffnen aber auch neue Optionen zum Einsatz digitaler Medien in der Grundschule. Wir möchten Sie weiterhin dazu ermutigen, die für Sie relevanten Themen aufzugreifen und damit ins Gespräch mit Ihrer Schulleitung, dem/der Datenschutzbeauftragten und mit Ihren Kolleginnen und Kollegen zu gehen.

Nicht zuletzt durch "Home-Schooling" und "Fernunterricht" haben daten-schutzrechtliche Aspekte in der Schul- und Bildungsarbeit nochmals verstärkt an Aufmerksamkeit gewonnen. Wir haben dies selbst durch die breite Resonanz auf die

Erstauflage unserer Handreichung unmittelbar erfahren, durch Rückfragen, Anregungen, Lob und Wünsche für weitere Erläuterungen.

Eine Auseinandersetzung mit datenschutzrechtlichen Fragestellungen von Videokoferenzsystemen und Online-Tools sowie ihre Auswirkungen auf die Organisation und Gestaltung von (Fern-)Unterricht würde jedoch den Umfang dieses Updates sprengen. Stattdessen streben wir an, zu diesem Themenbereich eine eigenständige Handreichung zu erarbeiten. Aktuelle Diskussionen und Raum für eigene Fragen finden Sie hier.

1. Änderung Schulgesetz

Unter den vielfältigen personenbezogenen Daten, die Schulen im Rahmen ihres Erziehungs- und Bildungsauftrags ohne Einwilligungserklärung erheben dürfen, waren bisher Bild- und Tonaufnahmen ausgeschlossen. Zum 1. August 2020 hat sich dies geändert:

- Bild- und Tonaufaufzeichnungen von Schülerinnen und Schülern dürfen ohne Einwilligungserklärung erstellt und verarbeitet werden.
- Bild- und Tonaufzeichnungen von Schülerinnen und Schülern dürfen zur Leistungsbeurteilung herangezogen werden. Bewertet werden darf hierbei nur die Form, nicht der Inhalt der Aufnahmen.
- Für beide Fälle gilt (vgl. § 115 Abs. 3a SchG):
  - Die Bild- und Tonaufnahmen müssen zur Erfüllung des schulischen Erziehungs- und Bildungsauftrags erforderlich sein.
  - Sie sind nicht verpflichtend.
  - Die Erziehungsberechtigten haben ein Widerspruchsrecht.

Im Folgenden möchten wir unter Hinzunahme der Hinweise zur Änderung des Schulgesetzes (SchG) zum 01.08.2020 des Kultusministeriums die Bedeutung dieser Gesetzesänderungen für die schulische Praxis erläutern:

Auf Einwilligungen zu Bild- und Tonaufnahmen kann u.U. verzichtet werden

Die geänderte Rechtsgrundlage führt zu einer Erleichterung beim Einsatz digitaler Medien in Schule und Unterricht, insbesondere von mobilen Endgeräten, die über Aufnahmefunktionen verfügen.

Möchte die Lehrkraft z.B. ein Videoprojekt in der Klasse durchführen, Sprachaufnahmen im Englischunterricht machen oder den Bewegungsablauf von Kindern im Sportunterricht aufzeichnen, so muss sie nicht mehr im Voraus Einverständniserklärungen der Erziehungsberechtigten einholen.

Diese Rechtsgrundlage gilt jedoch nur im Rahmen der Erfüllung des bezweckten Erziehungs- und Bildungsauftrags. Anschließend müssen die Aufnahmen gelöscht werden.

Sollen die Aufnahmen dauerhaft gespeichert (z.B. auf einem Speichermedium der Lehrkraft), weitergegeben (z.B. an die Klassengemeinschaft) oder veröffentlicht werden (z.B. Schulhomepage), müssen weiterhin entsprechende Einverständnis-erklärungen eingeholt werden (vgl. Punkte 2 und 3 der Mustervorlage ab S.18).

Achten Sie bitte auch auf die Einhaltung der übrigen erforderlichen Maßnahmen zum Datenschutz und zur Datensicherheit (Kapitel 4.2).

Bild- und Tonaufnahmen können zur Bewertung verwendet werden

Neu ist die Rechtsgrundlage für die Leistungsbeurteilungen von Bild- und Tonaufzeichnungen. Dies gilt jedoch nur für die Form — also die Aufzeichnung selbst —, nicht für ihren Inhalt. Beispielsweise dürfen aufgenommene Vorträge, Sportübungen oder schauspielerische Leistungen nicht bewertet werden, wohl aber die Machart von Audio- und Videoaufnahmen durch Schülerinnen und Schüler, z.B: Filmschnitt, Gestaltungsprinzipien der Kameraführung, Tonqualität.

Das Verbot, der Beurteilung von Aufzeichnungsinhalten erschließt sich dadurch, dass Bild- und Tonaufnahmen der eigenen Person nicht verpflichtend sind. Schülerinnen und Schüler können also der Aufnahme widersprechen, wodurch keine inhaltliche Bewertung möglich wird (vgl. folgender Absatz).

Die Löschfrist für bewertete Schülerarbeiten läuft bis Ende des darauffolgenden Schuljahres.

Freiwilligkeit und Widerspruchsrecht

Bild- und Tonaufnahmen im Schulunterricht sind möglich, aber nicht obligatorisch. Vielmehr müssen Lehrkräfte die Schülerinnen und Schüler dafür gewinnen, freiwillig bei Aufzeichnungen mitzumachen. Aufgrund der großen Neugierde von Kindern gegenüber audiovisuellen Medien und ihrem hohen Aufforderungscharakter werden Sie in den meisten Fällen keine Überzeugungsarbeit leisten müssen.

Zwar müssen Erziehungsberechtigte solchen Aufnahmen nicht mehr zustimmen — solange sie dem Bildungs- und Erziehungsauftrag dienen —, ihnen bleibt jedoch ein Recht auf Widerspruch. Die Schule muss über das Widerspruchsrecht informieren und Aufnahmen unterlassen, sollten die Eltern von ihrem Recht Gebrauch machen.

Wir empfehlen Ihnen, bei der Formulierung eines Informationsschreiben mindestens auf folgende Punkte hinzuweisen:

- Kontaktdaten der Schulleitung
- Art der Daten, die potentiell erhoben werden (z.B. Fotos, Videos, Tonaufnahmen)
- Freiwilligkeit der Aufnahmen, bei Widerspruch ist keine Angabe von Gründen notwendig, es entstehen keine Nachteile bei Widerspruch
- Information darüber, wer die Daten erhält bzw. nutzt, es erfolgt eine datensichere Speicherung - mit Angabe, wie Daten gespeichert werden
- Dauer der Datenspeicherung oder Information über Löschzeitpunkt.

Die unterschiedlichen Arten und Zwecke der Datenverarbeitungen sollten so konkret und verständlich wie möglich formuliert sein.

Weisen Sie auf die Potenziale von Bild- und Tonaufnahmen hin, z.B. motivationale Faktoren, fachdidaktische Potenziale, lebensweltliche Aspekte.

Idealerweise sprechen Sie das Thema auch persönlich an, z.B. im Rahmen eines Elternabends, an dem auch Nachfragen von Eltern direkt beantwortet werden können.

2. Komfortable Datenlöschung bei iPads

Es gibt gute Neuigkeiten für Schulen, die über eigene iPads verfügen, welche von unterschiedlichen Schülerinnen und Schülern benutzt werden. Um zu verhindern, dass Schülerinnen und Schüler auf erzeugte Daten fremder Nutzerinnen und Nutzer zugreifen konnten, war bisher ein zeitaufwendiges Verfahren notwendig: das Zurücksetzen aller Geräte (vgl. S. 23 und 24).

Seit Mitte 2020 gibt es die Möglichkeit, iPads mit temporären Sitzungen zu starten, nach deren Beendigung sämtliche generierte Daten automatisch gelöscht werden.

Shared iPads mit Gast-Zugang

Voraussetzungen für die Nutzung sind, dass die Geräte mindestens über iPadOS 13.4 verfügen, mit einem Mobile Device Management (MDM) verwaltet werden und die shared iPad-Funktion auf den Geräten aktiviert ist.

Nach erfolgter Einrichtung besteht die Möglichkeit, sich als anonymer Gast anzumelden. Die während des Betriebs im Gastmodus erzeugten Daten werden gelöscht, sobald das Gast-Konto wieder abmeldet wird. Bei dem Verfahren werden keine Daten in der iCloud gespeichert.

Einschränkend ist zu sagen, dass iPads im Gastmodus nicht über die Classroom-App angesteuert werden können.

Der Einsatz personalisierter Shared iPads, bei denen Benutzerkonten in der iCloud angelegt werden, wird aus datenschutzrechtlichen Gründen weiterhin nicht empfohlen, da eine Anmeldung an diesen Geräten nur über eine bei Apple verwaltete managed Apple-ID möglich ist, mit der Folge, dass alle in der Sitzung erzeugten Daten automatisch in die iCloud gelangen. Weitere Informationen zum Gastmodus finden Sie hier.

Was tun bei mehrtägigen Projekten?

Für Anwendungsszenarien, die nur eine Unterrichtseinheit umfassen ist dies eine ideale Lösung. Soll jedoch an längerfristigen Projekten gearbeitet sind zwei Szenarien denkbar:

- Die iPads werden für den gesamten Projektzeitraum geblockt und ausschließlich von den Schülerinnen und Schülern bedient, die an dem Projekt arbeiten. Währenddessen müssen die iPads eingeschaltet bleiben, sonst werden alle Daten gelöscht.
- Am Ende einer Sitzung werden bearbeitbare Projektdateien außerhalb des iPads gespeichert (z.B. schulische Nextcloud, Lehrer-iPad) und zu einem späteren Zeitpunkt wieder importiert und weiter bearbeitet. Informieren Sie sich bitte vorab, welche Apps das Speichern von bearbeitbaren Projektdateien erlauben. Hier eine Auswahl beliebter Apps: iMovie, Book Creator, Stop Motion Studio, Apple Office-Paket.

Ein kurzes Video-Tutorial zum Starten der temporären Sitzung im Gastmodus finden Sie hier.

Einführung

Digitale Medien sollen künftig selbstverständlicher Bestandteil des Schulunterrichts sein. Das ist das erklärte Ziel des *Bundesministeriums für Bildung und Wissenschaft*, um junge Menschen im digitalen Zeitalter zu einem selbstbestimmten und verantwortungsvollen Umgang zu befähigen.[2]

Tatsächlich ist das didaktische Potenzial insbesondere von Tablet-Computern groß, sofern sie pädagogisch sinnvoll eingesetzt werden. Sie sind leicht bedienbar und eröffnen – z.B. über Video- und Sprachaufnahmefunktion – neue Zugänge für das Lernen. Über das Internet kann auf Wissen außerhalb des Klassenzimmers zugegriffen oder mit Kindern der Partnerschule im Ausland kommuniziert werden. Auch sind verschiedene Formen des mobilen Lernens mit Tablets sehr gut möglich (z.B. auf dem Schulgelände, bei Exkursionen etc.).

Zugleich nehmen digitale Medien in der kindlichen Lebenswelt eine immer größere Rolle ein. Beispielsweise ist laut *KIM-Studie 2018* der Anteil der 8-9-Jährigen, die zumindest ab und zu online sind, auf knapp 60% gestiegen. Grundschulbildung hat vor diesem Hintergrund die Mediensozialisation der Kinder zu beachten und zu reflektieren – Bildungs- und Lernprozesse mit und über digitale Medien werden grundlegend auch für die Grundschulbildung.

Die Politik beginnt, Rahmenbedingungen zu setzen, durch die das Lernen mit und über digitale Medien gefördert wird. Seit 2016 ist die *Leitperspektive Medienbildung* im Bildungsplan des Landes Baden-Württemberg verankert. Auf Bundesebene verständigte sich im gleichen Jahr die Kultusministerkonferenz auf die Strategie *Bildung in der digitalen Welt*. Zudem können Schulträger bis 2022 über den *Digitalpakt* Sondermittel für die Ausstattung mit digitaler Technik beantragen.

Mit der zunehmenden Rolle digitaler Medien in der Schule erhöhen sich auch die Gefahren des Missbrauchs von Daten, die unweigerlich bei der Nutzung von Geräten, Programmen sowie des Internets entstehen und verbreitet werden. Daten, die im Kontext Schule und Unterricht entstehen, sind häufig sehr sensibel (z.B. Leistungsdokumentationen, Ordnungsmaßnahmen, Video- und Fotoaufnahmen). Durch einen Missbrauch dieser Informationen könnte für die Betroffenen ein hoher Schaden entstehen. Dies zeigt, dass ein funktionierender Datenschutz im Schulbereich immer mehr an Bedeutung gewinnt.

Bereits im Jahr 1983 hat das Bundesverfassungsgericht aus den Artikeln 1 und 2 des Grundgesetzes das Recht auf informationelle Selbstbestimmung abgeleitet. Jeder sollte demnach selbst über den Verbleib und die Verwendung der eigenen

2 vgl. Bundesministerium für Bildung und Wissenschaft - DigitalPakt Schule 2019: bmbf.de/de/wissenswertes-zum-digitalpakt-schule-6496.php

personenbezogenen Daten bestimmen können. Dieses Prinzip findet sich in der europäischen Datenschutz-Grundverordnung (DSGVO) wieder, welche im Jahr 2018 in Kraft trat und im Zusammenspiel mit nachgeordneten Bundes- und Landesgesetzen sowie Verordnungen den Rahmen für den Datenschutz an Schulen in Baden-Württemberg vorgibt. Die Vorschriften sind komplex und übertragen der einzelnen Schule und ihren Lehrkräften eine große Verantwortung. Hierdurch entstehen besondere Herausforderungen im schulischen Alltag. Beispielsweise dürfen Schülerinnen und Schüler ohne Einverständniserklärungen aller Beteiligten und ihrer Erziehungsberechtigten keine Videoaufnahmen im Rahmen des Unterrichts voneinander machen.

Die Autoren dieser Handreichung haben die Erfahrung gemacht, dass das Thema Datenschutz viele Lehrkräfte überfordert. Ein Teil der Lehrerinnen und Lehrer lässt sich entmutigen und setzt digitale Medien im Unterricht gar nicht erst ein, um keine Fehler zu begehen. Andere Lehrkräfte ignorieren mitunter datenschutzrechtliche Vorgaben – teilweise, weil sie davon ausgehen, dass ihnen die Vorschriften große pädagogische Spielräume nehmen. Es ist zu überlegen, welche Formen des Datenschutzes schulischen Situationen gerecht werden und wie Regelungen für den Unterrichtsalltag gefunden werden können, die sowohl Belange des Datenschutzes als auch den Unterrichtsalltag und die Belastungssituation von Lehrpersonen berücksichtigen.

Ziel dieser Handreichung ist, wesentliche datenschutzrechtliche Vorgaben für den Unterricht anhand von praktischen Fallbeispielen verständlich zu erklären. Dabei werden neben der Darstellung der rechtlichen Aspekte auch pädagogische Hinweise gegeben. Die Handreichung soll Lehrerinnen und Lehrern – insbesondere jenen an baden-württembergischen Grundschulen – Mut machen, digitale Medien im Unterricht einzusetzen. Datenschutz an der Schule ist wichtig und zugleich eine Bildungs- und Erziehungsaufgabe, um Kinder auf mögliche Gefahren des Datenmissbrauchs in verschiedenen Lebensbereichen aufmerksam zu machen. Wir sind der festen Überzeugung, dass in Zusammenhang mit Datenschutzfragen an Schulen klare Regeln, Abläufe und Zuständigkeiten dazu beitragen können, das Vertrauen von Lehrkräften, Eltern und auch Schülerinnen und Schülern in den Einsatz neuer Technologien zu gewinnen. Darüber hinaus braucht es eine verlässliche technische Infrastruktur, die von professionellem Personal in Stand gehalten wird, und qualifizierte pädagogisch-didaktische Unterstützung für die Lehrkräfte.

Aufbau der Handreichung

Im ersten Kapitel werden zunächst die **rechtlichen Grundlagen zum Datenschutz** an baden-württembergischen Schulen kurz umrissen. Hierbei erläutern wir die europäische Datenschutz-Grundverordnung und daraus folgende Prinzipien für die Datenverarbeitung.

Anschließend gehen wir detailliert auf die **informierte Einwilligung** der Sorgeberechtigten und eine für diese Handreichung erstellte Muster-Vorlage ein (zweites Kapitel). Zudem geben wir Tipps, wie die Vorlage in der Arbeit mit Eltern eingesetzt werden kann.

Im dritten Kapitel geben wir einen groben Überblick über mögliche **technische Szenarien an der Schule**, da diese mit datenschutzrechtlichen Fragen und Maßnahmen in einem unmittelbaren Zusammenhang stehen.

Anschließend erörtern wir im vierten Kapitel **drei zentrale Fragen zum Datenschutz**, die sich Lehrkräfte vor dem Einsatz digitaler Medien im Unterricht stellen sollten. Zudem werden die datenschutzrechtlichen Aspekte zum Einsatz von digitalen Medien im Unterricht und erforderliche Maßnahmen in einer Übersicht zusammengefasst.

Anhand von **zehn Fallbeispielen** wird in Kapitel fünf veranschaulicht, wie der Datenschutz in der Unterrichtspraxis der Grundschule eingehalten werden kann. Der thematische Schwerpunkt liegt auf der Anwendung von Tablets.

Im sechsten Kapitel geben wir einen Überblick über frei verfügbares **Unterrichtsmaterial zum Thema Datenschutz** für die Grundschule.

Im abschließenden **Fazit** (Kapitel 7) fassen wir die wichtigsten Informationen zusammen und geben einen **Ausblick** auf notwendige Schritte der Schulen, Schulverwaltung und Bildungspolitik. Im Anhang dieser Handreichung finden Sie Links zu hilfreichen Webangeboten.

Die einzelnen Kapitel bauen inhaltlich aufeinander auf, indem wir von eher abstrakten rechtlich-technischen Rahmenbedingungen auf konkrete Situationen zu sprechen kommen. Sie können diese Handreichung natürlich auch nicht-linear lesen, indem Sie bei einzelnen Fallbeispielen einsteigen und anschließend auf detaillierte Informationen weiter vorne im Text zurückgreifen.

Wichtiger Hinweis

Diese Handreichung ist nach bestem Wissen und Gewissen formuliert worden. Doch sowohl Gesetze und Verordnungen als auch Technologien wandeln sich fortlaufend.

Die Autoren erheben den Anspruch, die Hinweise zu Recht und Gesetz präzise und zutreffend darzustellen, eine aktuelle Rechtssicherheit kann jedoch nicht garantiert werden. Als Lehrerin und Lehrer sollten Sie daher den Einsatz digitaler Medien in Ihrem Unterricht immer wieder kritisch hinterfragen und gegebenenfalls an neue Anforderungen anpassen.

Zudem empfehlen wir Ihnen, im Rahmen der Planung Ihres Unterrichts mit digitalen Medien, bezüglich datenschutzrechtlicher Aspekte Rücksprache mit Personen der verschiedenen Ebenen der Schulverwaltung zu halten. Insbesondere Ihre Schulleitung und der bzw. die behördliche Datenschutzbeauftragte Ihrer Schule sind hierfür geeignete Ansprechpartner bzw. Ansprechpartnerinnen.

Entstehungskontext

Diese Handreichung ist im Rahmen des Entwicklungs- und Forschungsprojekts *Digitales Lernen Grundschule Stuttgart/Ludwigsburg (dileg-SL)* der *Pädagogischen Hochschule Ludwigsburg (PH)* entstanden. Das Projekt *dileg-SL* wurde im Zeitraum von 2016 - 2019 an der *PH Ludwigsburg* durchgeführt und von der *Deutsche Telekom Stiftung* gefördert. Im Rahmen von innovativen Seminarkonzepten entwickelten und erprobten Studierende Einsatzszenarien mit digitalen Medien in der Primarstufe der *Rosensteinschule* (Stuttgart), die Kooperationspartner im Projekt war. Aufgrund des vielseitigen Einsatzes von digitalen Medien in Unterrichtserprobungen spielte der Datenschutz eine wichtige Rolle. Im Laufe des Projekts entstanden ein umfassendes Datenschutzkonzept und drei wissenschaftliche Artikel, die sich mit datenschutzrechtlichen Fragen im Kontext der Nutzung von digitalen Medien an Hoch- und Grundschule befassten. Diese Broschüre möchte zentrale konzeptionelle Überlegungen und Erkenntnisse aus dem Projekt nun auch Lehrkräften verfügbar machen.

1. Kapitel: Rechtliche Grundlagen

Lehrerinnen und Lehrer kommunizieren im Kollegium über eMail, nutzen zur Unterrichtsvorbereitung Online-Videos, fotografieren mit ihrem Mobiltelefon ein Tafelbild: Digitale Medien sind mittlerweile im Alltag der Grundschule sehr präsent. Je mehr Funktionen und Einsatzmöglichkeiten die modernen Technologien bieten, desto mehr Daten werden verarbeitet – auch solche, die gesetzlich besonders geschützt sind.

Seit dem Inkrafttreten der europäischen **Datenschutz-Grundverordnung (DSGVO)**[3] im Jahr 2018 gibt es EU-weit klare Regeln, unter welchen Bedingungen sogenannte personenbezogene Daten erhoben und in welcher Weise diese dann genutzt werden dürfen. Die generellen Bestimmungen der DSGVO werden in den EU-Mitgliedsländern durch Landesgesetze präzisiert und auf landesspezifische Gegebenheiten konkretisiert. Für öffentliche Schulen finden sich solche spezialgesetzlichen Regelungen in den jeweiligen Landesdatenschutzgesetzen, Schulgesetzen und weiteren Verwaltungsvorschriften.

Die DSGVO greift die bisherigen datenschutzrechtlichen Grundprinzipien auf und schreibt sie fort. Die zentralen Prinzipien der DSGVO sind u.a.:

- Rechtmäßigkeit der Datenverarbeitung
- Betroffenenrechte
- Datensparsamkeit und Zweckbindung
- Datensicherheit
- Eingeschränkte Zulässigkeit der Übermittlung in Drittstaaten

Bevor wir uns jedoch in den nachfolgenden Absätzen diesen Prinzipien zuwenden, müssen wir zuerst zwei grundlegende Begriffe klären: *Datenverarbeitung* und *personenbezogene Daten*.

Datenverarbeitung

Der Weg der Datenverarbeitung beginnt immer dort, wo Informationen erstmals festgehalten bzw. erhoben werden. In der Folge werden Daten gespeichert, übermittelt oder versendet, genutzt, verändert und schlussendlich vernichtet bzw. gelöscht. Alle diese Schritte bezeichnet das Gesetz als **Datenverarbeitung**. Dabei wird weder zwischen *klassisch analogen* Daten (z.B. auf Papier) oder digitalen Daten, noch in der Art der Anwendung unterschieden (z.B. ob im Kopiergerät vervielfältigt oder auf USB-Stick übertragen).

3 dsgvo-gesetz.de

Nahezu alle Akteure in der Schule sind täglich mit Daten konfrontiert und an der Datenverarbeitung beteiligt: Die Schulleitung (z.B. bei der Meldung von Auslastungszahlen an Schulbehörden), Sekretariate und Hausservice (z.B. zur Organisation von Räumen), Lehrerinnen und Lehrer (z.B. bei der Erhebung von Noten), Schülerinnen und Schüler (z.B. bei Beobachtungsaufgaben) und Eltern (z.B. bei Krankmeldungen).

Personenbezogene Daten

Datenschutz bezieht sich nicht auf alle Daten, sondern nur auf die spezielle Kategorie der **personenbezogenen Daten**. Darunter fallen alle Angaben, die sich bestimmten, eindeutigen Personen zuordnen lassen. Personenbezogen ist eine Angabe dann, wenn ein Mensch mit einer Information direkt identifiziert werden kann. Hierzu gehören zum Beispiel Name, Wohnadresse, Telefonnummer, Foto- oder Stimmaufnahmen einer Person.

Darüber hinaus zählen aber auch weitere – zunächst unverfänglich erscheinende – Informationen, die mittelbar und in Kombination mit anderen Daten einen Rückschluss auf eine Person möglich machen, dazu (z.B. Geburtsdatum, besondere Körpermerkmale, Vereinsmitgliedschaften oder ausgefallene Hobbys).

In den Datenschutzgesetzen werden **besondere Arten personenbezogener Daten** nochmals gesondert behandelt, z.B. Angaben zur ethnischen Herkunft einer Person, deren religiöse Überzeugung, Angaben über Gesundheit oder Sexualleben. Diese Daten werden häufig auch als **besonders schützenswerte Daten** bezeichnet.

Im Schulbetrieb gehören insbesondere Beobachtungen, Bewertungen von Schülerleistungen, Berichte sowie Bild- und Videoaufzeichnungen aus Unterricht und Schulleben zur Kategorie *Personenbezogene Daten*. Weil Daten von Kindern mit höheren Risiken für deren Rechte und Freiheiten verbunden sind, werden diese generell als besonders schützenswert betrachtet (Art. 8 DSGVO; Erwägungsgrund 75). Alle Akteure in einer Schule tragen daher eine hohe Verantwortung bei der Verarbeitung personenbezogener Daten ihrer Schülerinnen und Schüler. Sie müssen in allen Schritten der Verarbeitung und Nutzung die Sicherheit gewährleisten und Risiken für die Betroffenen genau abwägen.

Rechtmäßigkeit der Datenverarbeitung

Das **Recht auf informationelle Selbstbestimmung** besagt, dass jeder Mensch über das Recht verfügt, über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen und selbst zu entscheiden, wann und wie bestimmte Informationen über seine persönlichen Lebensumstände veröffentlicht werden. Somit ist es grundsätzlich verboten, personenbezogene Daten zu erheben und zu verarbeiten. Nur auf Basis gesetzlicher Bestimmungen oder einer wirksamen Einwilligungserklärung der Betroffenen sind Ausnahmen von diesem Grundsatz möglich.

Jede Person ist jedoch immer Teil einer Gemeinschaft, deren übergeordnetes Allgemeininteresse gewisse Eingriffe in das Recht auf informationelle Selbstbestimmung erlaubt. Beispielsweise sind alle Menschen in Deutschland verpflichtet, gegenüber dem Finanzamt bestimmte personenbezogene Angaben zu machen. Für solche Einschränkungen müssen entsprechende Gesetze oder nachgeordnete Verwaltungsvorschriften erlassen werden, welche die Art und den Umfang der Datenverarbeitung klar und erkennbar regeln.

In Baden-Württemberg definiert die Verwaltungsvorschrift *Datenschutz an öffentlichen Schulen vom 5. Dezember 2014* dezidiert jedes einzelne personenbezogene Datum, welches von Schulen verarbeitet werden darf (z.B. Geburtsdatum des Schülers/der Schülerin, Kontaktdaten der Eltern oder Erziehungsberechtigten, Ordnungsmaßnahmen). Für Bild- und Sprachaufnahmen, die häufig beim Einsatz von digitalen Medien im Unterricht entstehen, ist diese Verwaltungsvorschrift dagegen keine Rechtsgrundlage.

Informierte Einwilligung

Immer dann, wenn kein spezielles Gesetz eine Verarbeitung personenbezogener Daten erlaubt, ist die **informierte Einwilligung** der einzig verbleibende Weg, um datenschutzkonform personenbezogene Daten zu verarbeiten. Vereinfacht ausgedrückt: Erst wenn eine betroffene Person über die geplante Datenverarbeitung informiert ist und dieser zustimmt, dürfen Daten erhoben und verarbeitet werden.

Eine solche Einwilligung erfordert bestimmte Inhalte und Angaben, um rechtlich wirksam zu sein. Grundsätzlich muss die Zustimmung als informierte Einwilligung erfolgen, d.h. die Eltern (bzw. Schüler ab dem 16. Lebensjahr) müssen in transparenter und verständlicher Form darüber informiert werden, in was sie einwilligen. Das Anschreiben zu einer Einwilligung sollte mindestens folgende Angaben beinhalten:

- die für die Datenverarbeitung **verantwortliche Person**, an welche die Eltern ihre Zustimmung richten (z.B. die Schulleitung);
- konkrete Angaben über **Zweck** (z.B. Trickfilm-Projekt), **Umfang** (z.B. Erhebungszeitraum) und **Art** (z.B. Foto- und Stimmaufnahmen) der erhobenen Daten sowie über den **weiteren Weg der Datenverarbeitung** (Ort und Dauer der Speicherung, Löschfristen);
- den ausdrücklichen Hinweis auf die **Freiwilligkeit** zur Mitwirkung an der Datenerhebung sowie das **Recht auf Auskunft, Widerruf und Datenlöschung**. Wichtig ist auch darauf hinzuweisen, dass aus einer Verweigerung oder einem Widerruf keine Nachteile für die Betroffenen bzw. die Kinder oder die Sorgeberechtigten selbst entstehen.

Weitere Informationen zur informierten Einwilligung entnehmen Sie bitte Kapitel 2.

Prinzipien der Zweckbindung und Datensparsamkeit

Das Gebot der **Zweckbindung** bedeutet, dass die erhobenen Daten tatsächlich nur für den eingangs zugesicherten Anlass bzw. Zweck verwendet werden (z.B. Videoaufnahmen für Feedbackgespräche im Sportunterricht). Jegliche davon abweichende, darüber hinausgehende Nutzung oder Weitergabe der Daten ist unzulässig. Sobald eine Aufgabe abgeschlossen ist und der Zweck der Datenerhebung erfüllt wurde, müssen die Daten gelöscht werden, es sei denn, eine Rechtsvorschrift erlaubt das weitergehende Vorhalten (z.B. bei Leistungsdokumentationen), oder die Eltern geben eine entsprechende Einwilligung (z.B. bei Fotos auf der Schulhomepage).

Der Grundsatz der **Datenvermeidung** bzw. **Datensparsamkeit** zielt darauf ab, so wenig personenbezogene Daten wie möglich zu erheben. Somit ist es unzulässig, alle auffindbaren Daten zu sammeln, um sie etwa für mögliche spätere Nutzungen schneller verfügbar zu haben. In Bezug auf das Beispiel aus dem Sportunterricht: Es sollte nicht die komplette Unterrichtsstunde aufgezeichnet und über längere Zeit aufbewahrt werden, wenn der Zweck der Aufnahmen sich ausschließlich auf Feedbackgespräche zu bestimmten Bewegungsabläufen bezieht. Auch hier greift das Prinzip der Zweckbindung: Sobald Daten nicht mehr gebraucht werden, sind sie zu löschen.

Anforderungen zur Datensicherheit

Die für den Datenschutz verantwortliche Person muss die Sicherheit der Daten hinsichtlich **Vertraulichkeit** und **Integrität** gewährleisten. Dies bedeutet, dass personenbezogene Daten vor unbefugter und unrechtmäßiger Weitergabe (Vertraulichkeit) sowie vor Verlust oder Schädigung (Integrität) – z.B. Bildmanipulationen – bewahrt

werden sollen. Die Schule muss sogenannte geeignete technische und organisatorische Maßnahmen umsetzen (z.B. Datenverschlüsselung, Pseudonymisierung[4], Bereitstellung eines Widerrufsformulars, klare Zuständigkeiten bei Auskunftsersuchen), um die Datensicherheit zu gewährleisten. Die technischen und organisatorischen Maßnahmen müssen angemessen sein, das heißt, sie berücksichtigen den Stand der Technik und das Risiko eines möglichen Schadens für die Betroffenen (z.B. bei Datenverlust). Je nach Schwere und Eintrittswahrscheinlichkeit eines Schadens muss die Datensicherheit auf ein akzeptables Niveau gehoben werden. Beispielsweise kann die Verschlüsselung von Daten im Falle des Verlusts des Datenträgers (z.B. USB-Stick) das Risiko enorm verringern, dass Unbeteiligte die gespeicherten Informationen einsehen könnten.

Übermittlung in Drittstaaten

Die Weitergabe von personenbezogenen Daten an **Dienstleister** (z.B. Cloud- oder App-Anbieter) **außerhalb der Europäischen Union** ist in der DSGVO nur unter bestimmten Bedingungen möglich, z.B. bei Vorliegen einer informierten Einwilligung, bei der die betroffene Person über die Risiken der Übermittlung aufgeklärt wurde. Das *Ministerium für Kultus, Jugend und Sport* (KM) legt diese Regelung in seinen Verwaltungsvorschriften[5] noch strenger aus. Demnach sind Datenübermittlungen nur an Dienstleister möglich, deren Sitz und Server in der EU liegen. Die Inanspruchnahme von beispielsweise US-amerikanischen Anbietern, wie *YouTube, WhatsApp* oder *Dropbox*, ist also auch dann untersagt, wenn die Betroffenen einer solchen Datenverarbeitung zustimmen würden.

Verantwortlichkeit

Grundsätzlich verantwortet die **Schulleitung** die angemessene Einhaltung der Datenschutzregelungen an der Schule. Da eine einzelne Leitungsperson nicht alle Aktivitäten der Mitarbeitenden überblicken kann, delegiert sie in der Regel die ordnungsgemäße Anwendung des Datenschutzes an die Lehrerinnen und Lehrer. Sie tragen die Verantwortung für die sachgemäße Berücksichtigung der Datenschutzbestimmungen im Rahmen ihrer Aufgaben. Darüber hinaus steht allen Akteuren ein Datenschutzbeauftragter bzw. eine Datenschutzbeauftragte beratend zur Seite. Für diese Aufgabe wird in der Regel eine fachkundige Lehrkraft benannt oder ein externer Datenschutzbeauftragter bzw. eine externe Datenschutzbeauftragte bestellt.

---

4 Bei der Pseudonymisierung wird ein Schülername durch eine Zahlenfolge oder einen Alias ersetzt, mit Hilfe einer Referenzliste kann der Personenbezug wieder hergestellt werden.

5 lehrerfortbildung-bw.de/st_recht/grund/verwalt/

Verzeichnis von Verarbeitungstätigkeiten

Eine der Aufgaben der Schulleitung im Kontext des Datenschutzes ist die Erstellung eines **Verzeichnisses für Verarbeitungstätigkeiten**. Darin ist zu dokumentieren, welche personenbezogenen Daten erhoben werden, wie diese gespeichert sowie verarbeitet und wie Löschfristen eingehalten werden. Generell ist dieses Verzeichnis für die gesamte schulische IT-Infrastruktur zu erstellen. Bei Projekten oder neuen Unterrichtsszenarien muss überprüft werden, ob eine Ergänzung der Unterlagen notwendig ist. Nähere Informationen finden Sie auf den Seiten der *Lehrerfortbildung Baden-Württemberg*.[6]

In dieser Handreichung können wir die Grundzüge der DSGVO nur ansatzweise wiedergeben. Eine ausführliche Erläuterung finden Sie in einer Veröffentlichung des Bundesdatenschutzbeauftragten[7]. Die *Medienberatung NRW* fasst die Prinzipien der DSGVO im Kontext von Schule in einer Broschüre[8] zusammen.

6 lehrerfortbildung-bw.de/st_recht/daten/ds_neu/verfahren
7 bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO1.html
8 schulministerium.nrw.de/docs/Recht/Datenschutz/Handreichung-Medienberatung/index.html

2. Kapitel: Informierte Einwilligung

Die informierte Einwilligung ist eine der bedeutsamsten Stellen im Datenschutz-Gefüge einer Schule. Sie bildet in vielen Fällen die Rechtsgrundlage, wenn beim Einsatz von digitalen Medien (z.B. Tablets) in Form von Fotografien, Video- und Sprachaufnahmen personenbezogene Daten von Schülerinnen und Schülern erhoben und verarbeitet werden. Neben den Kindern selbst haben dabei ihre Erziehungsberechtigten umfangreiche Beteiligungs- und Zustimmungsrechte (vgl. Kapitel 1).

Im Zusammenhang des Bildungs- und Erziehungsauftrags verfügen Lehrerinnen und Lehrer für bestimmte Daten über das Recht, diese ohne Einwilligung zu erheben (z.B. Noten). Hierüber haben Eltern bzw. betroffene Kinder kein Einwilligungsrecht. Das Unterrichten mit verschiedenen didaktischen Methoden und Medien ist aber überwiegend nicht gesetzlich geregelt, d.h. hierfür sind Einwilligungen erforderlich, wenn personenbezogene Daten erhoben werden.

Für das Szenario *Einsatz von digitalen Medien in der Grundschule* finden Sie im Folgenden eine auf diese Vorgaben abgestimmte Muster-Vorlage[9] zur Einwilligung. Sie ist vor dem Hintergrund der wissenschaftlichen Erkenntnisse und unserer Erfahrungen aus dem Entwicklungs- und Forschungsprojekt *dileg-SL* entstanden und versucht, die aktuellen gesetzlichen Vorgaben aufzugreifen und mit typischen schulischen Szenarien zu verbinden. Die Muster-Vorlage besteht aus zwei Komponenten: Zum ersten einem Anschreiben an die Eltern der betroffenen Kinder, das über den generellen Zweck der Datenverarbeitung informiert und Anlaufstellen benennt. Darauf folgt die Einwilligung im eigentlichen Sinne.

Die Vorgabe zur Differenzierung von Sachverhalten ist im Muster über eine gestufte Erläuterung nach Personenkreisen gelöst, die die erhobenen Daten empfangen oder Einsicht erhalten:

Im ersten Schritt (Stufe 1) entscheiden die Sorgeberechtigten, ob generell Aufnahmen ihrer Kinder in unterschiedlichen Zusammenhängen gemacht werden können. Vorher muss die Schule die konkreten Zwecke der Aufnahmen definieren und in die Vorlage eintragen.

Sofern die Eltern mindestens einer Form der Datenerhebung zugestimmt haben, können sie anschließend über weitere Arten der Datennutzung und Veröffentlichung entscheiden, ob Aufnahmen der Kinder innerhalb der Schule vorgeführt, an bestimmte Schulangehörige weitergegeben (Stufe 2) und über bestimmte Medien einer breiteren Öffentlichkeit zugänglich gemacht werden dürfen (Stufe 3).

9 Die Muster-Vorlage können Sie sich als Word-Datei unter folgendem Link downloaden: dileg-sl.de/muster-vorlage

Abschließend folgen Hinweise auf besondere Risiken im Zusammenhang mit der Veröffentlichung im Internet und Folgen des Widerrufs. Die Einwilligung bleibt für die Dauer der Schulzugehörigkeit gültig, sofern ihr nicht widersprochen wird.

Schulen sind unterschiedlich: In der Zusammensetzung der Schülerschaft, in den Strukturen und Abläufen des Unterrichts- und Schulbetriebs, wie Aufgaben und Verantwortlichkeiten organisiert sind, in Form verschiedener Kooperationen mit anderen Organisationen (Schulen, Vereine, Betriebe) und Personen (z.B. Eltern) usw. Rechtswirksame Einwilligungen müssen so gestaltet sein, dass sie zur Schule passen. Die Angaben in unserem Muster sollen hierzu als Anhaltspunkt dienen.

Wir wollen Sie ermutigen:

- Übernehmen Sie dieses Muster und jede andere Formularvorlage nicht ohne kritische Überprüfung und Überarbeitung. Erweitern Sie die Angaben um ggf. weitere Differenzierungen und kürzen Sie Angaben dort, wo diese auf Ihre Situation nicht zutreffen. Prüfen Sie z.B. mit welchen Kooperationspartnern Sie regelmäßig zusammenarbeiten und dabei gemeinsam personenbezogene Daten verarbeiten (Hochschulen, Einrichtungen der Kinder- und Jugendarbeit etc.).
- Bitten Sie Außenstehende (z.B. andere Schulen), übergeordnete Stellen (z.B. Schulamt) und Fachstellen (z.B. Medienzentrum) um Feedback zu Ihrem überarbeiteten Formularentwurf.
- Koordinieren Sie Abläufe und Teilaufgaben im Datenschutz zwischen Schulleitung und Fachbereichen. Erarbeiten Sie Informationsschreiben und Formulare im Team und nutzen Sie das Fach- und Erfahrungswissen im Kollegium.

Wesentlich für die Akzeptanz und die Umsetzung von Datenschutzvorgaben ist nach unseren Erfahrungen – jenseits formaler Dokumente – die Transparenz der Verfahren und das vertrauensvolle Verhältnis zu Eltern, in der Schülerschaft und im Kollegium an einer Schule. Dies wird in vielen Fällen durch persönliche Begegnungen, Gespräche, frühzeitige und fortlaufende Information ermöglicht. Wir empfehlen daher, die Frage der Einwilligung (in die Verarbeitung von personenbezogenen Daten) im Rahmen von Elternabenden zu besprechen, bei denen die Sorgeberechtigten zusätzliche Informationen erhalten, um bestimmte Zusammenhänge und Fachbegriffe begreifen und ihre Sorgen und Bedenken äußern zu können. In solchen Settings können außerdem Verständigungsschwierigkeiten mit Eltern, die der deutschen Sprache nur bedingt mächtig sind, durch einen persönlichen Kontakt in der Regel leichter überwunden werden. Beispielsweise kann eine Präsentation mit illustrierenden Fotos und Grafiken die Vermittlung von komplexen Sachverhalten erleichtern. Eventuell sind auch Eltern vor Ort, die bei der Übersetzung helfen können. Dieser Punkt ist besonders wichtig, da rechtliche Informationen oftmals in einer juristischen Sprache verfasst sind, die das Verstehen erschweren oder gar abschrecken.

Unwägbarkeiten könnten mit Eltern entstehen, die den Einsatz digitaler Medien im Unterricht skeptisch betrachten und die Schule als Schonraum begreifen, in dem Kinder vor dem vermeintlich schädlichen Einfluss digitaler Medien geschützt werden sollen. Die verantwortliche Lehrkraft sollte – neben den Potenzialen digitaler Medien – diese Bedenken kennen und sich mit ihnen intensiv auseinandersetzen. Hierfür lohnenswert ist ein Blick in die *Sammlung Argumente gegen das Digitale in der Schule*[10] und möglicher Gegenargumente von Beat Döbeli Honegger, Leiter des *Instituts für Medien und Schule* der *Pädagogischen Hochschule Schwyz*.

Schließlich gibt es Eltern, die für die Lehrkraft nicht *zu greifen sind* oder ihr Einverständnis nicht erteilen möchten. Die Inanspruchnahme des individuellen Rechts auf informationelle Selbstbestimmung muss die Lehrkraft respektieren und beim Einsatz von digitalen Medien im Unterricht stets berücksichtigen.

10 mehrals0und1.ch/Argumente

Muster-Vorlage Informierte Einwilligung

[*Name der Schule*]
[*Adresse der Schule*]
[*Datum*]

Bitte um Einwilligung zur Verarbeitung und Veröffentlichung von Foto-, Video- und Tonaufnahmen Ihres Kindes

Sehr geehrte Eltern,

junge Menschen müssen lernen, die Möglichkeiten der digitalen Medien (z.B. Computer, Tablets, Smartphones) zu nutzen. Daher sollen sie bereits an unserer Grundschule mit diesen Geräten üben und lernen. Die digitalen Medien ermöglichen neue Formen des Lehrens und Lernens, insbesondere mit Video-, Foto- und Tonaufnahmen. Wenn solche Aufnahmen von ihrem Kind entstehen, handelt es sich um eine Verarbeitung personenbezogener Daten. Entsprechend der gesetzlichen Datenschutzregelungen erfolgt diese Datenverarbeitung nur dann, wenn Sie hierzu vorher zustimmen. Die erhobenen personenbezogenen Daten werden ausschließlich von Lehrkräften, Mitarbeiterinnen und Mitarbeitern genutzt, die an unserer Schule tätig sind und diese Daten für ihre jeweiligen Aufgaben benötigen. Die erhobenen Daten werden nicht zur Bewertung oder Benotung herangezogen. Eine Weitergabe an Dritte ohne Ihre Zustimmung ist ausgeschlossen. Die Foto-, Video- bzw. Tondateien werden von uns gelöscht, sobald der jeweilige Zweck erfüllt ist.

Ihre Einwilligung ist freiwillig. Wenn Sie nicht zustimmen oder Ihre Einwilligung widerrufen, entstehen weder Ihnen noch Ihrem Kind Nachteile. Nach europäischer Datenschutz-Grundverordnung haben Sie jederzeit gegenüber der Schule ein Recht auf Auskunft über die Daten Ihres Kindes, zudem haben Sie ein Recht auf Berichtigung, Löschung, Einschränkung, Widerspruch und Datenübertragung. Wenden Sie sich hierzu oder bei generellen Fragen zum Datenschutz an [*Kontaktdaten der Schulleitung / Sekretariat*]. Unsere/n behördliche/n Datenschutzbeauftragte/n erreichen Sie unter [*Telefon und E-Mail-Adresse*]. Zudem steht Ihnen ein Beschwerderecht bei der uns zuständigen Datenschutzbehörde zu, dem Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg.

Bitte füllen Sie das Formular unten aus und bringen Sie es uns wieder zurück.

Mit freundlichen Grüßen
[*Schulleiterin / Schulleiter*]

Einwilligung “Foto-, Video- und Tonaufzeichnungen”

Betrifft mein Kind:

_____
[Name, Vorname, Geburtsdatum und Klasse der Schülerin / des Schülers]

1. Erhebung und lernbezogene Nutzung

Hiermit willige ich ein, dass von meinem Kind folgende personenbezogene Daten erhoben und verarbeitet werden können: (Bitte kreuzen Sie dort an, wo Sie zustimmen)

☐ Foto-, Video- und Tonaufnahmen im Klassenunterricht, um [*Zweck*].

☐ Foto-, Video- und Tonaufnahmen im Sportunterricht, um [*Zweck*].

☐ Foto-, Video- und Tonaufnahmen bei Schulaktivitäten und im Schulleben (z.B. Schülerfahrten, Schulfeiern, Tag der Offenen Tür), um [*Zweck*].

2. Schulinterne Vorführung und Weitergabe an Schulangehörige

In geeigneten Fällen wollen wir Unterrichtsergebnisse und Informationen über Ereignisse aus unserem Schulleben in der Schule vorführen oder an Schulangehörige (z.B. Eltern) weitergeben. Neben Klassenfotos kommen hier z.B. Foto- und Videoaufnahmen von Unterrichtsprojekten oder Schülerfahrten in Betracht.

Hiermit willige ich ein, dass von meinem Kind folgende personenbezogenen Daten vorgeführt oder weitergegeben werden können: (Bitte kreuzen Sie dort an, wo Sie zustimmen)

☐ Foto-, Video- und Tonaufnahmen aus der Klasse meines Kindes an die Eltern der Klasse.

☐ Vorführung von Foto-, Video- und Tonaufnahmen bei schulinternen Veranstaltungen (z.B. Jahresabschlussfeier, Lehrerverabschiedung).

☐ Fotoaufnahmen auf Aushängen und Plakaten auf dem Schulgelände.

3. Veröffentlichung

In geeigneten Fällen wollen wir im Rahmen der pädagogischen Arbeit oder von Schulveranstaltungen entstehende Foto-, Video- und Tonaufnahmen einer größeren Öffentlichkeit zugänglich machen. Neben Klassenfotos kommen hier z.B. Foto- und Videoaufnahmen von Unterrichtsprojekten, Wettbewerben, oder unser „Tag der Offenen Tür“ in Betracht.

☐ Fotoaufnahmen im Jahresbericht der Schule [*Empfängerkreis*]. Klassenfotos werden mit alphabetischen Namenslisten versehen, ansonsten werden Fotos keine Namensangaben beigefügt.

☐ Fotoaufnahmen in der örtlichen Tagespresse,

  ☐ inklusive Nennung von Name, Vorname und Klasse.

☐ Foto- Video- und Tonaufnahmen auf der Internet-Homepage der Schule unter [*https://www*],

  ☐ inklusive Nennung von Name, Vorname und Klasse.

Bei einer Veröffentlichung im Internet können die personenbezogenen Daten (einschließlich Fotos und Videos) jederzeit und zeitlich unbegrenzt weltweit abgerufen und gespeichert werden. Die Daten können damit etwa auch über so genannte Suchmaschinen (z.B. *Google*) gefunden werden. Dabei kann nicht ausgeschlossen werden, dass andere Personen oder Unternehmen die Daten mit weiteren im Internet verfügbaren personenbezogenen Daten verknüpfen und damit ein Persönlichkeitsprofil erstellen, die Daten verändern oder zu anderen Zwecken verwenden.

Wenn Sie Ihre Einwilligung zur Veröffentlichung widerrufen, werden die entsprechenden Daten zukünftig nicht mehr für die genannten Zwecke verwendet und auf der Internet-Homepage gelöscht. Die Rechtmäßigkeit der bis dahin erfolgten Datenverarbeitung wird nicht berührt. Bei Druckwerken ist der Widerruf dann wirksam, wenn ein neuer Druckauftrag erteilt wird.

_____

[Ort, Datum]

_____

[Unterschrift eines oder beider Erziehungsberechtigten]

Diese Vorlage wurde in Anlehnung an ein Formular des Kultusministeriums Baden-Württemberg (Stand: 07/2018) sowie Informationen des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg erstellt.

3. Kapitel: Technische Szenarien im Kontext des Datenschutzes

Datenschutzrechtliche Fragen und Maßnahmen stehen in einem unmittelbaren Zusammenhang mit technischen Voraussetzungen (z.B. Geräte, Software, Netzwerk), in deren Kontext Daten verarbeitet werden. Im Folgenden wollen wir eine Übersicht über mögliche Umsetzungsszenarien in Schule und Unterricht geben, da wir es als notwendig erachten, im Zusammenhang mit datenschutzrechtlichen Fragen beim Einsatz digitaler Medien, die technischen Grundlagen zu kennen.

3.1 Schulische IT-Infrastruktur

Im Folgenden geht es darum, Grundlagenwissen über die **schulische Informationstechnik (IT)** zu vermitteln. Selbstverständlich kann (und soll) es nicht die Aufgabe jeder Lehrkraft sein, das schulische Netzwerk einzurichten und zu betreuen. Dafür sind an Schulen die sogenannten *Netzwerkberaterinnen* und *Netzwerkberater* vorgesehen. Sie übernehmen – in Absprache mit der Schulleitung und dem IT-Dienstleister – die Betreuung der Geräte vor Ort. Die Einrichtung und Einbindung neuer Geräte sowie das Einspielen von Updates sind Aufgaben des Dienstleisters, der vom Schulträger beauftragt wird.

Die schulische IT-Infrastruktur besteht aus verschiedenen Elementen, wobei nicht alle hier aufgeführten Elemente zwingend in der Schule vorhanden sein müssen:

Netzwerk

Die Beschaffenheit des Schulnetzes ist abhängig von der Anzahl der Endgeräte, Nutzerinnen und Nutzern sowie den Nutzungsszenarien (z.B. WLAN für mobile Endgeräte). Es wird dringend empfohlen, eine strukturierte Verkabelung, also ein *professionelles* Netzwerk in der Schule zu installieren.

Das KM empfiehlt eine **dreistufige Netzwerkinfrastruktur** in der Schule, die eine saubere Trennung von Verwaltungs-, Lehrer- und Unterrichtsnetz gewährleistet.[11]

Hierdurch soll vermieden werden, dass Daten in falsche Hände gelangen und/oder manipuliert werden können, indem beispielsweise Noten durch unbefugte Dritte geändert werden. Schülerinnen und Schüler erhalten nur Zugriff auf das Unterrichts-

11 it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/Netztechnik+_+Netzbrief

netz, in dem keine Noten oder Beurteilungen abgelegt werden dürfen. Die Verarbeitung von kritischen personenbezogenen Daten geschieht im Lehrer- und im Verwaltungsnetz. Personalakten werden ausschließlich im Verwaltungsnetz verarbeitet, auf das wiederum die Lehrkräfte nicht zugreifen können.

Für IT-gestützte Formen des Unterrichts können PC-Räume, Computerinseln oder mobile Endgeräte wie Laptops oder Tablets genutzt werden, die in das Unterrichtsnetz eingebunden sind.

Server

Der (optionale) **Schulserver** kann verschiedene Funktionen übernehmen. In Bezug auf das Thema Datenschutz sind hier insbesondere folgende Aspekte zu nennen:

- **Benutzer- und Rollenkonzepte**: Eine Unterscheidung in verschiedene Benutzerrollen (z.B. *Lehrerin, Schüler*) ermöglicht es, dass verschiedene Zugriffsrechte vergeben werden. So erhält z.B. die *privilegierte* Lehrerin Zugriff auf Schülerverzeichnisse, während der Schüler nur seine eigenen Daten einsehen kann. Die Rolle *Lehrerin* hat in diesem Fall also mehr Möglichkeiten auf Daten zuzugreifen, als die Rolle *Schüler*.

- Über **individuelle Benutzerkonten**, durch die alle Anwenderinnen und Anwender einen (passwortgeschützten) Zugriff auf für sie freigegebene Ressourcen der Schul-IT erhalten, besteht die Umsetzung einer **Zugriffskontrolle**. Auf nicht freigegebene Inhalte (z.B. die Daten von anderen Nutzerinnen und Nutzern) kann nicht zugegriffen werden.

- Konzepte für die **Dateiablage**: Wie können Anwenderinnen und Anwender Daten ablegen, um später erneut darauf zugreifen zu können? Wie können Daten vor dem Zugriff anderer (unberechtigter) Nutzerinnen und Nutzer geschützt werden? Eine geordnete Verzeichnisstruktur und Benutzerrechte geben hierzu die Antworten.

Alternativ zum Schulserver werden (insbesondere in kleinen Schulnetzen) auch zentrale Festplattenspeicher, sogenannte NAS-Systeme (Network-attached Storage) betrieben. Hierbei sollte darauf geachtet werden, dass Daten einzelner Anwenderinnen und Anwender voneinander getrennt abgelegt werden und der Zugriff auf die Daten durch individuelle Kennwörter geschützt ist.

Endgeräte

Schulische Endgeräte sind stationäre Computer oder sogenannte *mobile devices* wie Laptops und Tablets, die ortsunabhängig eingesetzt werden können. Alle Schulgeräte sind Teil des pädagogischen Netzes. Sie können einzelnen Personen (z.B. Lehrer-Laptops), Schulklassen (z.B. Tablet-Klassensatz) oder allen Schülerinnen und Schülern sowie Schulbediensteten (z.B. PC-Räume) zugewiesen sein.

Zur Ergänzung der schulischen Ausstattung können Leihgeräte an der Schule eingesetzt werden. So kann eine Schule im Rahmen einer Projektarbeit einen Tablet-Koffer aus dem Kreismedienzentrum einsetzen.

Nutzungsszenarien

Der Einsatz eines Endgerätes kann über verschiedene **Nutzungsszenarien** geschehen. So können Geräte dauerhaft durch eine einzelne Schülerin/einen einzelnen Schüler (1:1) aber auch im (unterrichts-)stündlichen Wechsel von beliebig vielen Schülerinnen und Schülern (1:N) genutzt werden.

1:1-Zuordnung – jede/r hat ein eigenes Gerät
In diesem Fall ist ein Endgerät exklusiv einer Nutzerin oder einem Nutzer zugeordnet und wird nicht mit anderen geteilt.

Um die Daten vor dem Zugriff anderer Personen zu schützen, sollte das Gerät über einen Authentifizierungsmechanismus (Kennwortschutz, PIN, o.ä.) geschützt werden. Noch ist die 1:1-Ausstattung an baden-württembergischen Schulen allerdings eine absolute Ausnahme.

1:N-Zuordnung – ein Gerät wird von vielen genutzt
Im Falle der Gerätenutzung durch einen größeren Personenkreis ist darauf zu achten, dass die Datenbereiche der einzelnen Nutzerinnen und Nutzer voneinander getrennt sind.

Wenn dies technisch nicht möglich ist, müssen die Geräte nach jeder Nutzung bzw. vor jeder Übergabe an andere Schülerinnen und Schüler **zurückgesetzt** werden. Dies ist aktuell bei *Android*-Tablets und *iPads* der Fall[12] Zwar bietet *Apple* mit *shared iPads* die Möglichkeit, Daten von Schülerinnen und Schülern zu trennen, indem individuelle Datenspeicher auf den *iPads* angelegt werden. Diese Lösung darf jedoch an baden-württembergischen Schulen aus Datenschutzgründen nicht eingesetzt werden, da *shared iPads* Daten in die *iCloud* (*Apple-Cloud*, deren Server in den USA stehen) überträgt.

12 it.kultus-bw.de/site/pbs-bw-new/get/params_Dattachment/4695606/Hinweise-mobile-Endgeraete-im-Unterricht.pdf, S. 5f

Zurücksetzen bedeutet in diesem Fall, dass alle Daten, die bei der Nutzung gespeichert und anschließend von anderen Nutzerinnen und Nutzern eingesehen werden könnten, gelöscht werden. In der Regel sind schulische Tablets in ein sogenanntes *Mobile Device Management* (MDM) eingebunden, mit dem eine drahtlose Verwaltung der Geräte möglich ist. Die Administratorin bzw. der Administrator des MDMs kann das Zurücksetzen der Tablets mit wenigen Klicks in Gang setzen. Allerdings ist mit diesem Prozess eine langwierige Neuinstallation der Geräte verbunden. Daher werden Tablets in der Regel über Nacht zurückgesetzt. Manche Hersteller von MDM-Systemen arbeiten gerade an Lösungen, die es ermöglichen sollen, Daten zu löschen, ohne ein Gerät neu zu bespielen. Dies ist technisch jedoch nicht einfach umsetzbar. Es ist zu hoffen, dass es in Zukunft einfachere Verfahren der Datenlöschung geben wird.

Geräte können jedoch auch über die Systemeinstellungen manuell zurückgesetzt werden. Dies ist empfehlenswert, um Benutzerdaten zu löschen, bevor Leihgeräte wieder zurück an den Ausleiher gegeben werden.

Konzepte der Dateiablage

Daten, die im Unterricht anfallen, können auf verschiedenen Datenspeichern abgelegt werden:

- schulinterner Massenspeicher (z.B. Schul-Server, NAS)
- schulische private Cloud (von extern erreichbarer Cloudserver im Verantwortungsbereich der Schule)
- Endgerät, auf dem die Daten erzeugt werden
- externe Datenträger (z.B. USB-Stick, externe Festplatte)
- Cloudserver von externen Dienstleistern (Public Cloud)

Bei den **schulinternen Geräten** (Server, NAS, Endgeräte und private Cloud der Schule) ist – wie oben bereits ausgeführt – darauf zu achten, dass die Daten durch eine Zugriffskontrolle geschützt werden. Dies bedeutet zum einen, dass dafür gesorgt werden sollte, dass die technische Infrastruktur, wie Server oder Datenspeicher, nicht frei zugänglich sondern in verschlossenen (Server-)Räumen vorgehalten werden. Zum anderen sollte der Zugang in schulische IT-Systeme durch Benutzerkonten und zugehörige Kennwörter gesichert sein.
Exemplarisch für die *paedML Linux* (Schulische IT-Infrastrukturlösung des Landes Baden-Württemberg) ist das Dokument *Integration von iOS-Tablets*[13], in dem unter anderem beschrieben wird, wie Dateien, die im Unterricht auf *iPads* erstellt werden, in die Homeverzeichnisse[14] der *paedML* gespeichert werden können.
Ein gesonderter Fall der (lokalen) Datenablage sind **externe Datenträger**. Sobald die

13 lmz-bw.de/netzwerkloesung/produkte-paedml/paedml-linux/downloads/#howtos
14 Dateiablagen, in denen die einzelnen Benutzerinnen und Benutzer volle Schreib- und Leserechte haben.

Lehrkraft die von ihr benötigten Daten beispielsweise auf einem USB-Stick verarbeitet, muss eine Verschlüsselung personenbezogener Daten stattfinden. Nur so kann gewährleistet werden, dass Daten, im Fall eines Verlusts des Datenträgers, nicht durch Unbefugte eingesehen werden können. Nähere Informationen zur Verschlüsselung finden Sie auf den Seiten der *Lehrerfortbildung Baden Württemberg.*[15]

Bei der Verwendung **externer Datenspeicher** ist zu prüfen, ob der Dienstleister den Kriterien der DSGVO entspricht. Nur wenn sichergestellt werden kann, dass die Datenverarbeitung rechtskonform ist, darf ein solches Angebot genutzt werden. Mit dem jeweiligen Dienstleister ist in diesem Zusammenhang ein *Vertrag zur Auftragsdatenverarbeitung* zu schließen (vgl. Kapitel 3.2).

Verschiedene Adressatinnen und Adressaten

Daten können von **unterschiedlichen Adressatinnen und Adressaten** eingesehen und ggf. bearbeitet werden. Im schulischen Kontext sind das folgende Gruppen:

- Schülerinnen und Schüler
- Lehrkräfte
- Eltern
- außerschulische Kooperationspartner (z.B. bei Projekten)
- Öffentlichkeit (z.B. Fotos auf der Schulhomepage)
- externe Dienstleister (z.B. IT-Dienstleister, Anbieter von Cloud-Service, App-Hersteller)

Aus datenschutzrechtlicher Sicht ist unbedingt sicherzustellen, dass für jegliche Speicherung und Weitergabe von personenbezogenen Daten die informierte Einwilligung der Betroffenen vorliegt. Die Rechtsgrundlagen für Ausnahmen sind in den Verwaltungsvorschriften des KM geregelt.[16]

Nutzungsordnung

Aus datenschutzrechtlicher Perspektive ist die Einführung einer **Nutzungsordnung**, in der Regelungen für die Nutzung der schulischen IT-Infrastruktur festgelegt werden, empfehlenswert. Sie wird durch die Schülerinnen und Schüler (bzw. deren Erziehungsberechtigten) akzeptiert und bildet somit eine vertragliche Vereinbarung über die Nutzung der schulischen IT-Infrastruktur, die u.a. Regelungen zum Datenschutz und zur Datensicherheit enthalten.
Diese Maßnahme sollte jährlich für alle Schülerinnen und Schüler erneuert werden, sofern schulische IT-Infrastruktur im Unterricht genutzt wird. Mehr Informationen zu

15 lehrerfortbildung-bw.de/st_recht/daten/ds_neu/technik/usb
16 lehrerfortbildung-bw.de/st_recht/grund/verwalt

diesem Thema finden Sie im Web-Portal der *Lehrerfortbildung Baden-Württemberg*.[17]

Das eigenhändige Unterschreiben einer Nutzungsordnung kann bei Schülerinnen und Schülern das subjektive Bewusstsein für Datenschutz steigern. Zustimmungserklärungen zu Nutzungsordnungen sollten jedoch nicht im luftleeren Raum stattfinden, sondern stets in Prozesse der Medienbildung eingebunden sein, um die (eher abstrakten) Regelungen für die Schülerinnen und Schüler mit Leben zu füllen. Weitere Informationen und Unterrichtsmaterialien entnehmen Sie bitte Kapitel 6.

3.2 Zusammenarbeit mit externen Dienstleistern

Gerade an Grundschulen ist häufig keine hinreichende technische Ausstattung vorhanden. Fehlende Endgeräte, eine mangelhafte IT-Infrastruktur sowie die fehlende technische Betreuung, die an weiterführenden Schulen durch die Person der Netzwerkberaterin bzw. des Netzwerkberaters erfolgt, erschweren die Bedingungen für IT-gestützten Unterricht. Zur Kompensation dieser Mängel nutzen Lehrkräfte häufig **Angebote externer Dienstleister**:

- **Leihgeräte**: Fehlende Geräte werden für den Unterricht gemietet, z.B. bei einem Kreismedienzentrum.
- **Cloud-Services**: Statt Daten der Schülerinnen und Schüler auf dem (häufig nicht vorhandenen) Schulserver abzulegen, erfolgt die Speicherung von Arbeitsergebnissen in der Datencloud. Bekannte Cloud-Anbieter sind z.B. *Dropbox, OneDrive, MagentaCLOUD*. In ähnlicher Art und Weise lassen sich auch **Web-Plattformen** (z.B. *YouTube, Padlet, Flickr*) verwenden.
- **Apps**: Dieses Szenario betrifft alle Schulen. Sowohl auf schuleigenen als auch schulfremden Geräten arbeiten Schülerinnen und Schüler mit Apps, bei deren Nutzung in der Regel Daten anfallen, die – je nach Anbieter – teilweise auf die Server des App-Herstellers übertragen werden können. Manchmal ist so eine Datenübertragung auf den ersten Blick jedoch nicht ersichtlich.

Allen drei Szenarien ist gemein, dass Daten aus dem Unterricht die schulische Infrastruktur verlassen und von externen Dienstleistern verarbeitet werden könnten. Dies bedeutet, dass sich die Schule vor der Nutzung der Dienste mit den jeweiligen Anbietern zusammensetzen muss, um ...

1. … zu prüfen, dass das **Angebot des Herstellers datenschutzkonform** ist.
Zu klärende Fragen hierbei sind:

17 lehrerfortbildung-bw.de/st_recht/form/netz

- Welche Daten werden erhoben?
- In welchem Land stehen die Server?
- Wann werden die Daten gelöscht?
- Kann sichergestellt werden, dass die Daten nicht an Dritte weitergegeben werden?
- Kann sichergestellt werden, dass die Daten nicht für Werbezwecke ausgewertet werden?

2. … einen **Vertrag zur Auftragsdatenverarbeitung (ADV)** abzuschließen, in welchem Antworten auf oben genannte Fragen festzuschreiben sind. Auftraggeberin ist die Schule bzw. die Schulleitung, die weiterhin die datenschutzrechtliche Verantwortung trägt und gegenüber den Betroffenen auskunftspflichtig ist.

Das KM empfiehlt ausdrücklich:

- ausschließlich mit Dienstleistern zusammenzuarbeiten, die ihren Sitz im Geltungsbereich der DSGVO – also innerhalb der EU – haben. Dabei ist auch auf Unterauftragnehmer zu achten.
- sich im Vertrag schriftlich zusichern zu lassen, dass keine Verarbeitung personenbezogener Daten außerhalb der EU erfolgt und auch keine Daten an Stellen außerhalb der EU (auch nicht an staatliche Stellen, Behörden) übermittelt werden.

Nicht gestattet ist daher die Nutzung von Cloud-Dienstleistungen der großen amerikanischen Anbieter wie Apple, *Microsoft* oder *Google*. Das KM empfiehlt auf seiner Internetplattform alternative Anbieter.[18]

Generell problematisch ist die **datenschutzrechtliche Prüfung von Apps**. Das KM nennt in seinem *Leitfaden für die datenschutzkonforme Auswahl und Nutzung von Apps*[19] insgesamt 25 Punkte, welche Schulen vor der Nutzung einer App im Unterricht prüfen sollten. Unter anderem wird dringend empfohlen, die Allgemeinen Geschäftsbedingungen sowohl vor der Erstverwendung als auch nach jedem Update auf Veränderungen vollständig zu prüfen. Zeitlich und fachlich können Schulen dies kaum leisten. Wir empfehlen stattdessen, regelmäßig eine Risikoabwägung zu treffen in Verbindung mit den pädagogischen Zielen, die mit der Nutzung einer App verfolgt werden. Zuerst sollten Sie überlegen, ob durch die Verwendung einer App, überhaupt ein pädagogischer oder arbeitsorganisatorischer Mehrwert entsteht. Anschließend sollten Sie abschätzen, was für ein Schaden den Kindern entstehen könnte, wenn sie eine bestimmte App nutzen, und wie hoch das Risiko ist, dass dieser Schaden eintreten könnte. Ein potentielles Risiko ist immer dann gegeben, wenn Apps Daten von den verwendeten Geräten abgreifen. Daher erachten wir Apps, welche personenbezogene Daten ausschließlich lokal auf dem Endgerät ablegen als grundsätzlich weniger problematisch.

18 it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/Onlinespeicheranbieter
19 it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/mobile

Jedoch kann auch die Nutzung von eher *datenhungrigen* Apps – sogar solchen von außereuropäischen Anbietern – datenschutzrechtlich konform sein, sofern keine personalisierten Geräte verwendet und keine eindeutigen personenbezogenen Daten preisgegeben werden. Beispielsweise könnte eine Klasse kollaborativ mithilfe der US-amerikanischen App *Padlet* ein virtuelles Tafelbild über den Buchstaben A erstellen. Im Rahmen eines solchen Mini-Projekts könnten die Kinder *nebenbei* dafür sensibilisiert werden, was personenbezogene Daten sind, warum man sie schützen sollte und wie datensparsam gearbeitet werden kann.

Wichtiger Hinweis: Eine ADV ist ein komplexer und zeitaufwendiger Vorgang. Das KM stellt zwar geeignete Hinweise und Formulare zur Verfügung[20], für deren Verständnis und Anwendung ist jedoch rechtliches und IT-Fachwissen notwendig. Sie sollten sich daher im Voraus gut überlegen, ob die Schule über entsprechende fachliche und zeitliche Ressourcen verfügt, um einen Vertrag zur ADV erarbeiten und abschließen zu können. Im Zweifel sollten Sie lieber auf die Nutzung externer IT-Dienstleistungen verzichten.

3.3 Private Lehrergeräte

Da viele Schulen technisch nicht ausreichend ausgestattet sind, bringen Lehrkräfte häufig **private Datenverarbeitungsgeräte** (z.B. Tablet, Laptop, Digitalkamera) in die Schule mit, um sie im Unterricht oder anderen Schulveranstaltungen einzusetzen. Zudem möchten viele Lehrerinnen und Lehrer personenbezogene Daten ihrer Schülerinnen und Schüler (z.B. Klassenarbeiten, Bewertungen, Videos) auf privaten Datenspeichern ablegen (z.B. USB-Sticks, externe Festplatten, Heim-PC), um damit außerhalb der Schule arbeiten zu können.

Rechtlich ist dies insoweit relevant, als dass die Schule ihre datenschutzrechtlichen Verpflichtungen auf privaten Geräten nicht erfüllen kann. Sie hat z.B. keinen Einfluss darauf, ob Lehrkräfte Daten in einer Cloud synchronisieren und hierdurch sensible Informationen die Schule verlassen könnten. Zudem bergen externe Datenspeicher wie USB-Sticks, Festplatten oder mobile Endgeräte durch Verlust die erhöhte Gefahr, dass Daten durch unberechtigte Dritte eingesehen werden.
Rechtlich geregelt ist die *Nutzung privater Datenverarbeitungsgeräte durch Lehrkräfte* in der Verwaltungsvorschrift *Datenschutz an öffentlichen Schulen (Abschnitt I, Nr. 11)* sowie in der *Anlage 1*.[21]
Generell muss der Einsatz privater Geräte für dienstliche Zwecke durch die Schulleitung genehmigt werden, sobald zur Erfüllung schulischer Aufgaben personenbezogene Daten verarbeitet werden. Hierzu muss die Lehrkraft einen **Antrag auf Nutzung privater Datenverarbeitungsgeräte für dienstliche Zwecke**[22] stellen. Darin verpflich-

20 it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/Datenschutz+an+Schulen
21 landesrecht-bw.de
22 lehrerfortbildung-bw.de/st_recht/form/dv

tet sie sich u.a. zu folgenden **technischen und organisatorischen Geräte- und Datensicherungsmaßnahmen**:

- Zugangssicherungen für Geräte (z.B. Passwort, PIN, Fingerabdruck)
- Verwendung eines aktuellen Betriebssystems und regelmäßige Durchführung von Updates
- Einrichtung einer Firewall und eines Virenscanners
- Pseudonymisierung und Verschlüsselung der Daten sowie regelmäßige Datensicherungen (Backups)
- Insbesondere bei mobilen Endgeräten: Deaktivierung von Cloud-Services

Wir sind der Auffassung, dass die skizzierten Maßnahmen mit grundlegenden – für den heutigen Lehrerberuf unverzichtbaren – IT-Anwendungskompetenzen umsetzbar sind. Daher möchten wir Sie ausdrücklich dazu ermutigen, sich mit der Nutzung eines privaten Endgeräts (soweit Ihnen eines zur Verfügung steht) für schulische Angelegenheiten auseinanderzusetzen.[23] Gemeinsam mit der Schulleitung kann im Einzelfall entschieden werden, welche Datensicherungsmaßnahmen umgesetzt werden müssen. Beispielsweise im Fall von mobilen Endgeräten verschlüsselt das Apple-Betriebssystem *iOS* alle Dateien automatisch. Selbst durch den Ausbau der integrierten Festplatte könnten Dritte nicht auf die Daten zugreifen. Eine aktive Verschlüsselung seitens der Nutzerinnen und Nutzer ist daher nicht notwendig.
Weitere Informationen zur Nutzung von privaten Lehrergeräten finden Sie auf den Seiten der *Lehrerfortbildung Baden-Württemberg*.[24]

Schülergeräte (BYOD)

Einige Schulen setzen auf das Konzept **Bring Your Own Device (BYOD)**, bei dem Schülerinnen und Schüler eigene Geräte, insbesondere Smartphones, in die Schule bringen und im Unterricht als Lernwerkzeug einsetzen. Auch wenn BYOD für weiterführende Schulen große Potenziale hat, ist sein Einsatz in der Primarstufe fragwürdig. Nur ein geringer Teil der Grundschulkinder besitzt eigene mobile Computer (z.B. Smartphone, Tablet, Laptop). Es wäre daher pädagogisch zweifelhaft, wenn Grundschulen durch BYOD den Druck auf Kinder und Eltern erhöhen würden, ein Endgerät anzuschaffen. Zudem können Schülerinnen und Schüler wegen der Lernmittelfreiheit nicht verpflichtet werden, eigene Geräte in der Schule einzusetzen. Auf Grund dieser Überlegungen wird im weiteren Verlauf dieser Handreichung nicht auf datenschutzrechtliche Aspekte des BYOD-Konzepts eingegangen. Einige datenschutzrechtliche Hinweise zu BYOD finden Sie auf den Seiten der *Lehrerfortbildung Baden-Württemberg*.[25]

23 Am Ende dieser Handreichung finden Sie Links zu Fortbildungsmöglichkeiten.
24 lehrerfortbildung-bw.de/st_recht/daten/faq_ds, vgl. Abschnitt: Fragen zur Nutzung privater IT-Ausstattung
25 lehrerfortbildung-bw.de/st_recht/daten/checkl/aufnahme/

4. Kapitel: Übersicht zu datenschutzrechtlichen Aspekten und erforderlichen Maßnahmen

In den ersten drei Kapiteln haben wir die rechtlichen und technischen Grundlagen des schulischen Datenschutzes im Kontext von digitalen Medien skizziert. Im weiteren Verlauf dieser Handreichung möchten wir möglichst kompakt darlegen, was dies für Ihren Unterrichtsalltag als Lehrerin und Lehrer bedeutet. Im ersten Unterkapitel zeigen wir Ihnen anhand von drei Leitfragen, wie Sie rasch prüfen können, ob Sie technisch-organisatorische Datenschutzmaßnahmen ergreifen müssen und stellen die möglichen Szenarien kurz dar. Im zweiten Unterkapitel skizzieren wir technisch-organisatorische Maßnahmen, die Sie als Lehrkraft durchführen können, um die datenschutzrechtlichen Prinzipien einzuhalten.

4.1 Datenschutzrechtliche Aspekte im Unterricht

Wir empfehlen Ihnen, sich folgende drei Fragen zu stellen, bevor Sie digitale Medien in der Schule einsetzen, da anhand der Antworten notwendige Handlungsschritte (technische oder organisatorische Maßnahmen) ersichtlich werden:

1 *Entstehen personenbezogene Daten beim Einsatz von digitalen Medien?*

Zunächst einmal stellt sich die Frage, welche Art von Daten verarbeitet werden: Handelt es sich überhaupt um personenbezogene Daten?

Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die sich konkreten Personen eindeutig zuordnen lassen können. Im Rahmen von Schule und Unterricht sind dies u.a.: Namen, Adressdaten, Geburtstage, Foto-, Ton-, und Videoaufzeichnungen von Menschen und (Leistungs-)Bewertungen.

Der Verarbeitung von personenbezogenen Daten sind strenge Grenzen gesetzt.

Erforderliche Maßnahme (sofern nicht durch Verordnungen geregelt):
» Informierte Einwilligung einholen

Keine personenbezogene Daten

Nicht personenbezogene Daten sind Informationen, die sich weder mittel- noch unmittelbar konkreten Personen zuordnen lassen können und sind datenschutzrechtlich unerheblich.

Keine Maßnahme erforderlich

Allerdings ist nicht immer eindeutig zu klären, wann ein Datum nicht personenbezogen ist. Auch scheinbar unverfängliche Daten (z.B. Browserverlauf, Wohnort, Lieblingsfarbe) könnten – sinnvoll miteinander kombiniert – auf eine eindeutige Person verweisen.

2 *Datenerzeugung: Mit welchen Geräten werden die personenbezogenen Daten erstellt und zwischengespeichert?*

Um den Prozess der Datenverarbeitung in der täglichen Unterrichtspraxis verständlich abzubilden, unterscheiden wir zwischen Datenerzeugung (Frage 2) und Datenübermittlung (Frage 3). Sobald Nutzerinnen und Nutzer Daten mit einem Aufnahme- bzw. Eingabegerät (z.B. Tablet, PC, Digicam) erzeugen, werden sie dort auch (zwischen)gespeichert. Entscheidend ist, ob es sich um schuleigene oder private Geräte handelt. Rechtlich ist dies insoweit relevant, als dass die Schule datenschutzrechtliche Verpflichtungen auf externen Geräten nicht erfüllen kann.

Schulgeräte

Schulgeräte sind in aller Regel ins pädagogische Netz eingebunden. Insoweit kann die Schule kontrollieren, wie Daten verarbeitet und von wem sie eingesehen werden können. Wenn jedoch Geräte klassenübergreifend genutzt werden (1:N), könnten Schülerinnen und Schülern unberechtigten Zugang zu personenbezogenen Daten Dritter erlangen.

Erforderliche Maßnahme:
» Bei 1:N-Nutzung: Datenlöschung vor Weitergabe der Geräte an andere Schülerinnen und Schüler

Private Lehrergeräte

Der Einsatz **privater Lehrergeräte** im Unterricht birgt bestimmte datenschutzrechtliche Risiken, da die Geräte in aller Regel nicht dem Standard der schulischen IT entsprechen, sondern individuell durch ihre Besitzerinnen und Besitzer konfiguriert werden. Die Schule hat keinen technischen Einfluss darauf, ob über diese Geräte z.B. Daten in eine Cloud synchronisiert werden. Auf diese Weise könnten sensible personenbezogene Daten die Schule verlassen.

Erforderliche Maßnahmen:
» Antrag auf Nutzung privater Datenverarbeitungsgeräte für dienstliche Zwecke
» Gewährleistung der Sicherheit von Daten und privaten Endgeräten

Leihgeräte

Im Gegensatz zu Privatgeräten hat die Schule einen vergleichsweise großen Einfluss darauf, wie Daten auf **Leihgeräten** (z.B. vom Kreismedienzentrum) verarbeitet werden. Problematisch wäre jedoch der Fall, sollten personenbezogene Daten auf Leihgeräten nach ihrer Rückgabe verbleiben.

Erforderliche Maßnahme:
» Datenlöschung durch Zurücksetzen der Geräte

3 *Datenübermittlung: Wohin werden personenbezogene Daten übertragen? Wer hat Zugang zu den Daten?*

Vom Aufnahme- bzw. Eingabegerät, auf dem Daten entstehen, werden diese in der Regel auf andere Datenträger übertragen (z.B. von einem Tablet auf eine externe Festplatte, von einem Laptop in die Cloud). Bei der Verarbeitung personenbezogener Daten muss die Schule die Kontrolle über den Datenfluss behalten. Es muss nachvollziehbar sein, wo Daten verarbeitet und von wem sie eingesehen werden können. Es muss außerdem gewährleistet sein, dass die Daten fristgerecht gelöscht werden. Bei lokalen Datenspeichern (z.B. PC, Tablets, USB-Sticks) ist dies (mit grundlegenden Anwendungskompetenzen) gut umsetzbar. Bei der Nutzung von Dienstleistungen von Drittanbietern müssen umfassende Kriterien erfüllt werden.
Für die Veröffentlichung und Übermittlung von Daten an konkrete Personen (z.B. Vorführungen von Schülerarbeiten, Schulhomepage, Weitergabe an Eltern) bedarf es einer Einwilligung durch die Betroffenen.

Schulinterne Datenverarbeitung

Technische Schulinfrastruktur

Eine zentrale Datenspeicherung findet meist auf dem **Schulserver** oder einer **schuleigenen NAS** statt. Über persönliche Benutzerkonten kann eine Zugangskontrolle zu den Daten umgesetzt werden. Sofern die vorgeschriebenen IT-Standards eingehalten werden, müssen keine weiteren Maßnahmen erfolgen.

Keine Maßnahme erforderlich

Private Datenspeicher von Lehrkräften

Ob personenbezogene Daten auf **privaten Lehrergeräten** (z.B. Tablet, PC, USB-Stick) erzeugt oder übertragen werden, ist datenschutzrechtlich gleich zu bewerten, da die Geräte nicht dem Standard der schulischen IT entsprechen, sondern individuell durch ihre Besitzerinnen und Besitzer konfiguriert werden. In beiden Fällen sind umfassende technisch-organisatorische Maßnahmen durch die Lehrkraft umzusetzen.

Erforderliche Maßnahmen:
» Antrag auf Nutzung privater Datenverarbeitungsgeräte für dienstliche Zwecke
» Gewährleistung der Sicherheit von Daten und privaten Endgeräten

Externe Server

Apps & Cloudspeicher

Der Übermittlung und Speicherung von personenbezogenen Schülerdaten auf **Server externer Anbieter von Apps, Cloud-Services** etc. sind durch das KM sehr enge Grenzen gesetzt. Sie sind nur unter folgenden Bedingungen möglich:

1. Das genutzte Angebot ist DSGVO-konform.
2. Sowohl der Firmensitz als auch die Server, auf denen die Daten abgelegt werden, befinden sich im Geltungsbereich der DSGVO, also der EU.
3. Die Schule schließt mit der betreffenden Firma einen Vertrag zur Auftragsdatenverarbeitung.

Mögliche erforderliche Maßnahmen:
» Vertrag zur Auftragsdatenverarbeitung
» Unterlassung der Verarbeitung personenbezogener Daten

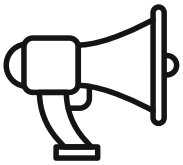
(Schul-) Öffentlichkeit

Datenspeicher von Schülerinnen und Schülern sowie ihren Eltern; schulöffentliche Aufführungen

Häufig besteht der Wunsch, dass personenbezogene Daten von Schülerinnen und Schülern (z.B. Klassenfahrtfotos, Schüler-arbeiten) allen Klassenmitgliedern und ihren Eltern zugänglich gemacht werden. Wir empfehlen hierfür die Verwendung von privaten USB-Sticks. Dabei ist zu bedenken, dass solch eine Weitergabe nur mit ausdrücklicher Zustimmung aller Betroffenen rechtens ist. Gleiches gilt bei schulöffentlichen Aufführungen von personenbezogenen Daten (z.B. das Zeigen eines Schülervideos beim Sommerfest).

Erforderliche Maßnahme:
» Informierte Einwilligungen einholen

Veröffentlichung von Daten



Werden personenbezogene Daten im Rahmen der schulischen Öffentlichkeitsarbeit verwendet (z.B. Schulhomepage, öffentliche Schulfeste, Pressearbeit), gelangen diese in die Öffentlichkeit. Diese Form der Datenverarbeitung benötigt eine gesonderte Form der Einwilligung, da die weitere Verbreitung dieser Daten nicht mehr gesteuert werden kann.

Erforderliche Maßnahme:
» Informierte Einwilligung einholen mit explizitem Hinweis im Informationsteil, dass Daten im Internet möglicherweise uneingeschränkt verbreitet werden

4.2 Erforderliche Maßnahmen

Im Folgenden präsentieren wir eine Übersicht über technisch-organisatorische Maßnahmen, die notwendig sind, um in bestimmten Einsatzszenarien von digitalen Medien die datenschutzrechtlichen Prinzipien einzuhalten.

Informierte Einwilligung

Die Verarbeitung von personenbezogenen Daten, welche nicht durch Gesetze oder Verordnungen geregelt ist, erfordert die **informierte Einwilligung** der Betroffenen bzw. deren gesetzlichen Vertreterinnen und Vertreter. Folgende Angaben muss eine Einwilligung beinhalten: Zweck, Umfang und Art der Datenverarbeitung, verantwortliche Person, Speicherort, Löschfristen, Hinweise auf Freiwilligkeit sowie Recht auf Auskunft, Widerruf und Datenlöschung.

Antrag auf Nutzung privater Datenverarbeitungsgeräte für dienstliche Zwecke

Der Einsatz von Lehrergeräten im Unterricht und die Verarbeitung personenbezogener Schülerdaten auf privater Hardware (z.B. PC, USB-Stick, Laptop) muss bei der Schulleitung beantragt werden. Mit ihrer Unterschrift verpflichten sich Lehrerinnen und Lehrer, die Sicherheit des privaten Geräts und der darauf gespeicherten personenbezogenen Daten zu gewährleisten.

Geräte- und Datensicherheit

Wenn Lehrkräfte personenbezogene Schülerdaten auf privaten Endgeräten und Datenträgern verarbeiten, müssen sie insbesondere sicherstellen, dass Unbefugte nicht auf diese Daten zugreifen können. Hierzu gehören u.a. folgende Maßnahmen:

- Zugriffssperren (z.B. Passwörter, Benutzerkonten)
- Maßnahmen zur Sicherheit der IT (z.B. Updates, Virenschutz, Firewall)
- Deaktivierung von Cloud-Diensten
- Datensicherheit (z.B. Pseudonymisierung, Verschlüsselung)

Datenlöschung (inkl. Zurücksetzen von Geräten)

Personenbezogene Daten müssen regelmäßig gelöscht werden, z.B. wenn

- ihr Erhebungszweck erfüllt ist (z.B. Projektende).
- Löschfristen ablaufen.
- die informierte Einwilligung widerrufen wird.
- personenbezogene Daten auf gemeinschaftlich genutzten Geräten (1:N-Szenario), die keine individuelle Benutzerkennung ermöglichen, durch andere Nutzerinnen und Nutzer eingesehen werden könnten. Im Fall von Tablets geschieht die Löschung durch das **Zurücksetzen** der Geräte.

Vertrag zur Auftragsdatenverarbeitung

Bevor schulfremde Dienstleister personenbezogene Daten einsehen und verarbeiten können, muss die Schule mit dem Anbieter einen Vertrag zur **Auftragsdatenverarbeitung** abschließen. Darin werden u.a. folgende Dinge vertraglich geregelt:

- Gegenstand und Umfang der Datenverarbeitung
- Unterauftragsverhältnisse mit Dritten (Dienstleister des Dienstleisters)
- Technische und organisatorische Maßnahmen der Datenverarbeitung

Wenn ein solcher Vertrag abgeschlossen wird, bleibt die datenschutzrechtliche Verantwortung weiterhin bei der Schule, die gegenüber den Betroffenen auskunftspflichtig ist. Verboten sind Verträge mit Anbietern, deren Firmensitz oder Server sich außerhalb des Geltungsbereichs der DSGVO – also der EU – befinden.

Unterlassung der Verarbeitung personenbezogener Daten

Sollten angemessene Maßnahmen zum Datenschutz nicht umsetzbar sein, empfehlen wir Ihnen, von der Verarbeitung personenbezogener Daten abzusehen.

5. Kapitel: Fallbeispiele aus der Schul- und Unterrichtspraxis

In zehn konkreten Fallbeispielen möchten wir Ihnen nun darlegen, wie Sie digitale Medien in Schule und Unterricht datenschutzkonform einsetzen können. Bei der Beurteilung der Szenarien gehen wir anhand der drei Leitfragen aus Kapitel vier vor. Nach rechtlichen Hinweisen geben wir jeweils eine medienpädagogische Einschätzung zu jedem Fallbeispiel ab. Beginnen möchten wir mit der folgenden **Ausgangssituation**:

Frau Müller ist Klassenlehrerin an der Grundschule. Seit neuestem besitzt ihre Schule einen eigenen Tablet-Koffer mit 16 Geräten. Die Tablets werden gemeinschaftlich verwendet, technisch können jedoch keine individuellen Benutzerprofile angelegt werden. Darüber hinaus betreibt die Schule einen eigenen Server, auf dem u.a. Kinder und Lehrkräfte Daten ablegen können und die Schulhomepage gehostet wird. Frau Müller besitzt einen Heim-PC, hat vor kurzem auch ein eigenes Tablet gekauft und möchte nun erste Erfahrungen mit mobilen, digitalen Medien im Grundschulunterricht machen.

Übersicht Fallbeispiele

Fallbeispiel 1:
Mit Sprachaufnahmen im Fremdsprachenunterricht arbeiten

Situationsbeschreibung
Im Englischunterricht sollen alle Kinder an ihrer Aussprache arbeiten. Frau Müllers Plan ist, dass die Schülerinnen und Schüler mit Hilfe der Schultablets einen selbst entwickelten Dialog zum Thema „Uhrzeit" aufnehmen und ihn später der Klassengemeinschaft präsentieren.

Datenschutzrechtliche Aspekte	Erforderliche Maßnahmen
1  Stimmaufnahmen sind **personenbezogene Daten**.	 Frau Müller benötigt **informierte Einwilligungen in Tonaufnahmen**. Kinder, deren Eltern nicht zustimmen, dürfen keine Stimmaufnahmen machen.
2  Die Schülerinnen und Schüler verwenden **Schulgeräte** (Tablets).	 Frau Müller setzt die **Tablets nach dem Unterricht zurück**, bevor sie von einer anderen Klasse verwendet werden.

Medienpädagogische Einschätzung
Die Potenziale von Tablets im Fremdsprachenunterricht sind besonders vielfältig. Hierzu zwei Beispiele:
1. Wenn Schülerinnen und Schüler sich beim Sprechen oder Vorlesen aufnehmen und die Aufzeichnung später anhören, bekommen sie – wie in einem *Verzögerten Spiegel* – ein unmittelbares Feedback des Arbeitsprozesses. Indem sie ihre eigene Leistung bewerten, trainieren sie ihre Selbstwahrnehmung und können ihre Lernfortschritte nachvollziehen.
2. Unsichere und leistungsschwächere Schülerinnen und Schüler trauen sich häufig nicht, vor der Klasse in einer Fremdsprache zu sprechen, da sie befürchten, Fehler zu machen und ausgelacht zu werden. Mithilfe eines Tablets können sie jedoch so lange an einer Aufnahme arbeiten, bis sie die Sicherheit haben, ihr Arbeitsergebnis über

Beamer und Lautsprecher klassenöffentlich zu zeigen. Dadurch werden diese Schülerinnen und Schüler für andere sichtbar und können Selbstwirksamkeit erfahren.
Problematisch wird es, sollten nicht alle Eltern den Sprachaufnahmen im Unterricht zustimmen. Die Lehrkraft sollte in solchen Fällen genau prüfen, wie verhindert werden kann, dass Kinder ohne Einwilligung ausgeschlossen oder benachteiligt werden, z.B. könnten sich diese Kinder gegenseitig ein Feedback zu ihren sprachlichen Leistungen geben.

Fallbeispiel 2:
Tablet als Dokumentenkamera einsetzen

Situationsbeschreibung
Frau Müller möchte ihr privates Tablet als Dokumentenkamera im Unterricht einsetzen, um über den Beamer mitgebrachte Insekten vergrößert zeigen zu können.

Datenschutzrechtliche Aspekte	Erforderliche Maßnahmen
1  Es werden **keine personenbezogenen Daten** verarbeitet.	Es sind keine Maßnahmen erforderlich.

Medienpädagogische Einschätzung
Gegenüber herkömmlichen Dokumentenkameras haben Tablets bei der Veranschaulichung von Inhalten Vorteile.Lehrkräfte können Inhalte aus Büchern und Zeitschriften nicht nur für alle Schülerinnen und Schüler sichtbar machen, sondern auch – wenn die Inhalte vorher abfotografiert werden – (mit einem Eingabestift) mit handschriftlichen Notizen versehen.
Die Mobilität der Tablets macht einen flexiblen Einsatz möglich und eröffnet zusätzliche didaktische Szenarien, z.B. bei der Veranschaulichung von Einstellungsgrößen und Perspektiven der Filmsprache: Der Effekt der Froschperspektive kann live an einem Schüler demonstriert werden. Durch Neigung und Veränderung des Abstands zum Schüler kann die Lehrkraft die Wirkung der Froschperspektive verstärken oder abschwächen. Darüber hinaus können Prozesse (z.B. Experimente) foto- und/oder videografisch festgehalten und (z.B. in Zeitlupe) wiedergegeben werden.
Zahlreiche Apps bieten zudem interaktive Simulationen zu unterschiedlichen Fachinhalten an (z.B. die *iOS-App Der menschliche Körper*). Zu beachten ist, dass für diese Anwendungen ein Tablet in eine geeignete technische Infrastruktur, bestehend aus Beamer und Streaming-Adapter (z.B. *Apple TV, Chromecast*), eingebunden sein muss.

Fallbeispiel 3:
Bewegungsabläufe im Sportunterricht filmen

Situationsbeschreibung
Im Sportunterricht möchte Frau Müller die Schülerinnen und Schüler Seilspringen üben lassen. Sie plant, die Kinder mit ihrem privaten Smartphone zu filmen und ihnen anschließend anhand der Aufnahmen Feedback zu geben.

Datenschutzrechtliche Aspekte	Erforderliche Maßnahmen
1  Die Videoaufnahmen der Kinder sind **personenbezogene Daten**.	 Frau Müller benötigt **informierte Einwilligungen in Videoaufnahmen im Sportunterricht**. Kinder deren Eltern nicht zustimmen, dürfen nicht gefilmt werden.
2  Frau Müller nutzt die Kamerafunktion ihres **privaten Smartphones**.	 Mit Hilfe eines **Antrags auf Nutzung privater Datenverarbeitungsgeräte für dienstliche Zwecke** holt Frau Müller die Zustimmung der Schulleitung ein. Frau Müller gewährleistet die **Sicherheit der Daten** auf ihrem Smartphone, z.B. verhindert sie, dass Videos (automatisch) in eine Cloud geladen werden. Spätestens nach der Unterrichtsstunde **löscht** Frau Müller **alle Videos**, da der Zweck der Aufzeichnung mit dem mündlichen Feedback erfüllt wurde.

Medienpädagogische Einschätzung

Durch wiederholtes Ansehen der Aufzeichnungen – insbesondere in Zeitlupe – bekommen Schülerinnen und Schüler einen neuen Zugang, sich ihrer Bewegungstechniken bewusst zu werden und diese anschließend verbessern zu können. Solche Videoaufnahmen sollten besonders sensibel behandelt werden, da Kinder im Sportunterricht häufig knappe und körperbetonte Bekleidung tragen. Beachten Sie bitte auch, Videoaufnahmen aus dem Sportunterricht nicht als Grundlage für eine Bewertung zu verwenden.
Sollten einzelne Kinder nicht gefilmt werden dürfen, muss sichergestellt werden, dass auch diese Kinder ein adäquates Feedback zu ihren Leistungen bekommen.

Fallbeispiel 4:
Weiterleitung personenbezogener Daten an Eltern und ihre Kinder

Situationsbeschreibung
Frau Müller fährt mit ihrer Klasse ins Schullandheim und möchte den Aufenthalt mit ihrer Smartphone-Kamera dokumentieren. Zu Hause will sie die Fotos auf ihren PC übertragen und die schönsten Bilder in einem Ordner zusammenstellen. Sie überlegt, die Fotoauswahl allen Eltern weiterzuleiten.

Datenschutzrechtliche Aspekte

1

Fotoaufnahmen, auf denen Kinder erkennbar sind, sind **personenbezogene Daten**.

Erforderliche Maßnahmen

Frau Müller benötigt **informierte Einwilligungen in Fotoaufnahmen von Schulaktivitäten**. Kinder, deren Eltern nicht zustimmen, darf sie nicht fotografieren.

Datenschutzrechtliche Aspekte	Erforderliche Maßnahmen
2  Frau Müller nutzt die Kamerafunktion ihres **privaten Smartphones** und überträgt die Fotos auf ihren **PC**.	 Mit Hilfe eines **Antrags auf Nutzung privater Datenverarbeitungsgeräte für dienstliche Zwecke** holt Frau Müller die Zustimmung der Schulleitung ein. Frau Müller gewährleistet die **Sicherheit der Daten** auf ihrem Smartphone und PC, z.B. verhindert sie, dass Videos (automatisch) in eine Cloud geladen werden.
3  Frau Müller möchte eine Auswahl der Fotos **an alle Eltern weiterleiten**.	 Frau Müller benötigt von allen Eltern, die Fotoaufzeichnungen erlaubt haben, zusätzlich die **informierte Einwilligung**, dass Abbildungen des eigenen Kindes an andere Eltern weitergegeben werden dürfen. Fotos, auf denen Kinder zu erkennen sind, deren Eltern einer Weitergabe jedoch nicht zugestimmt haben, sortiert Frau Müller aus. Frau Müller **löscht** die Fotos nach der Übergabe an die Eltern, sofern keine andere Regelung vereinbart wurde.

Medienpädagogische Einschätzung
Fotos spielen sowohl für Kinder als auch deren Eltern eine herausragende Rolle als Medium des Selbstausdrucks, des Erinnerns, der körperlichen Selbstdarstellung etc. Vermutlich wäre es für die meisten Kinder und Eltern nicht nachvollziehbar, wenn sie von der Klassenfahrt keine Erinnerungsfotos besitzen würden. Ebenso besteht häufig der Wunsch, dass besondere Schülerergebnisse (z.B. Trickfilme), die personenbezogene Daten mehrerer Kinder enthalten, an die Eltern weitergegeben werden.

Gleichzeitig muss das Recht auf informationelle Selbstbestimmung beachtet werden, sofern Einzelne mit einer Weiterleitung nicht einverstanden sind.
Daher sollten Sie möglichst frühzeitig gemeinsam mit den Eltern (z.B. beim Elternabend) offen diskutieren, ob personenbezogene Daten der Schülerinnen und Schüler weitergegeben werden können. Vertrauen könnte dadurch geschaffen werden, wenn Sie versichern, dass keine bloßstellenden Darstellungen herausgegeben werden. Umgekehrt sollten sich die Eltern darauf einigen, dass keine Daten an Dritte weitergeben werden – sie sollten insbesondere nicht über soziale Netzwerke geteilt werden.

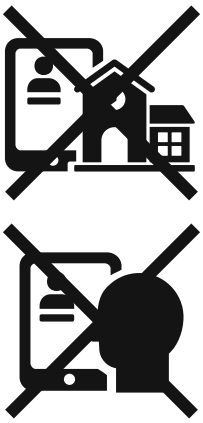
Fallbeispiel 5:
Darf die Begleitperson Fotos vom Schulausflug machen?

Situationsbeschreibung
Frau Müller plant, mit ihrer Klasse eine Aufführung im kommunalen Theater zu besuchen. Herr Meier – Vater einer Schülerin – hat sich bereit erklärt, als Begleitperson mitzukommen. Gerne würde er mit seiner Kamera Fotos vom Schulausflug machen.

Datenschutzrechtliche Aspekte	Erforderliche Maßnahmen
1  Fotoaufnahmen, auf denen Kinder erkennbar sind, sind **personenbezogene Daten**.	 Frau Müller benötigt **informierte Einwilligungen in Fotoaufnahmen von Schulaktivitäten**. Kinder, deren Eltern nicht zustimmen, dürfen nicht fotografiert werden.

Datenschutzrechtliche Aspekte **Erforderliche Maßnahmen**

2



Bei der Kamera von Herrn Meier handelt es sich weder um ein **Schul**- noch um ein **Lehrergerät**.

Frau Müller bittet Herrn Meier, Fotos ausschließlich von seiner Tochter zu machen, da die Schule weder Einfluss auf die Konfiguration seiner Kamera noch auf die weitere Verarbeitung personenbezogener Daten anderer Kinder hat. Zwar könnte Frau Müller Herrn Meier ihre private Kamera zur Verfügung stellen, sofern sie für die Verwendung des Geräts eine Erlaubnis der Schulleitung eingeholt hat. Für die Weiterleitung der Fotos wären jedoch informierte Einwilligungen der Eltern aller betroffenen Schülerinnen und Schüler notwendig.

Medienpädagogische Einschätzung

Fotos der eigenen Kinder sind im Familienalltag selbstverständlich geworden und nehmen für Eltern einen hohen Stellenwert ein. Einige Väter und Mütter gehen jedoch fahrlässig mit Bildern eigener und fremder Kinder um, wenn sie unreflektiert und übermäßig in Sozialen Medien geteilt werden (*Sharenting*). Zum einen sollten Eltern für einen kritischen Umgang mit personenbezogenen Daten sensibilisiert werden, zum anderen sollten Lehrkräfte und Schulen klare Regeln aufstellen. Ein absolutes Fotografieverbot bei Schulveranstaltungen würde jedoch die elterlichen Bedürfnisse nicht angemessen berücksichtigen. Wir schlagen daher vor, z.B. bei Einschulungsfeiern, die Eltern zu Beginn der Veranstaltung zu bitten, keine Fotos zu machen, jedoch am Ende einen Rahmen zu schaffen, in dem alle Kinder und Eltern freiwillig zusammen kommen können, um Fotos zu schießen.[26]

26 Vgl. Nr. 16 unter lehrerfortbildung-bw.de/st_recht/daten/faq_ds/

Fallbeispiel 6:
Kreativ-produktive Apps einsetzen und datenschutzkonform auswählen

Situationsbeschreibung
Frau Müller möchte im Deutschunterricht die App Green Screen by Do Ink verwenden. Mit Hilfe dieser App sollen die Schülerinnen und Schüler in Kleingruppen Videomontagen erstellen, in denen sie sich an ihrem anstehenden Sommerferienort befinden und von dort berichten. Frau Müller prüft die Funktionalitäten und die Datenschutzerklärung der App.

Datenschutzrechtliche Aspekte	Erforderliche Maßnahmen
1  Bei den geplanten Foto- und Videoaufnahmen, die mit der App gemacht werden sollen, handelt es sich um **personenbezogene Daten**.	 Frau Müller benötigt unterschriebene **informierte Einwilligungen in die Anfertigung von Videoaufzeichnungen im Unterricht**. Kinder, deren Eltern nicht zustimmen, dürfen sich nicht filmen lassen.
2  Die App ist auf **schuleigenen Geräten** installiert. Laut der Datenschutzerklärung (Stand 21.08.2019) lädt die App keine Video-, Foto- oder Audiodaten auf externe Server.	 Frau Müller **setzt** nach dem Einsatz **die Tablets zurück**, bevor sie an eine andere Klasse ausgehändigt werden.

Datenschutzrechtliche Aspekte	Erforderliche Maßnahmen
3  Laut der Datenschutzerklärung (Stand 21.08.2019) greift das Unternehmen auf bestimmte Daten zu: Absturzberichte der App und Nutzerkennzahlen (z.B. Version des verwendeten Tablets, Version des Betriebssystems).	Da die Schulgeräte laufend von unterschiedlichen Schülerinnen und Schülern genutzt werden, können die erhobenen Daten nicht personalisiert werden. Daher ist die schulische Nutzung der App *Green Screen by Do Ink* datenschutzrechtlich vermutlich unbedenklich.

Medienpädagogische Einschätzung

Aus medienpädagogischer Sicht sind besonders die kreativ-produktiven Apps für Schule und Unterricht geeignet. Als kreativ-produktiv bezeichnen wir Apps, welche es erlauben, fremde oder eigens erstellte multimediale Inhalte zu (v)erarbeiten.

Kinder können auf diese Weise Geschichten erzählen, Themenhefte erstellen oder Rollenspiele aufzeichnen. Am Ende des Arbeitsprozesses steht ein Produkt, das mit einem bestimmten Maß an Kreativität und Selbstbestimmtheit entstanden ist und daher besonders motivierend für die Lernenden sein kann.

Zudem eignen sich kreativ-produktive Apps für die Kleingruppenarbeit, in denen Kinder soziale Kompetenzen erwerben und einüben können. Bewährt haben sich neben der App *Green Screen by Do Ink*, die Trickfilm-App *Stop Motion Studio* und *Book Creator*, mit der Multimedia-eBooks erstellt werden können.

Schülerinnen und Schüler ohne elterliche Einwilligung können im Rahmen von Gruppenarbeiten Aufgaben übernehmen, bei denen sie voraussichtlich nicht gefilmt werden, z.B. Kamerakind sein. Zudem sollte die Lehrkraft offen in der Klasse kommunizieren, dass bestimmte Kinder nicht zu filmen sind. Eine absolute Garantie, dass einzelne Kinder gegen diese Regel nicht verstoßen (sowohl unwissentlich als auch mit Vorsatz) kann es nicht geben.

Weitere Informationen zur datenschutzkonformen App-Auswahl entnehmen Sie bitte Kapitel 3.2.

Fallbeispiel 7:
Ein Schülervideo auf *YouTube* veröffentlichen

Situationsbeschreibung
Im Sachunterricht möchte Frau Müller mit ihrer Klasse ein Video über die Klimaerwärmung produzieren, in welchem die Kinder im szenischen Spiel u.a. Möglichkeiten aufzeigen, wie man den eigenen CO2-Fußabdruck verringern kann. Das Video wird auf Frau Müllers privatem Tablet erstellt. Sie überlegt, das fertige Video auf YouTube zu veröffentlichen.

Datenschutzrechtliche Aspekte	Erforderliche Maßnahmen
1  Videoaufnahmen von Schülerinnen und Schülern sind **personenbezogene Daten**.	 Frau Müller benötigt **informierte Einwilligungen in Videoaufnahmen**. Kinder, deren Eltern nicht zustimmen, dürfen nicht gefilmt werden.
2  Frau Müller erstellt und speichert das Video auf ihrem **privaten Tablet**.	 Frau Müller stellt einen **Antrag auf Nutzung privater Datenverarbeitungsgeräte für dienstliche Zwecke** bei der Schulleitung. Frau Müller gewährleistet die **Sicherheit der Daten** auf ihrem Smartphone und PC, z.B. verhindert sie, dass Videos (automatisch) in eine Cloud geladen werden. Frau Müller **löscht die Daten** spätestens zum Ende des nächsten Schuljahrs, sofern sie mit den Eltern keine anderweitige Vereinbarung getroffen hat.

Datenschutzrechtliche Aspekte	Erforderliche Maßnahmen
3  Frau Müller plant, die Trickfilme auf *YouTube* zu **veröffentlichen**.	 Das Hochladen von personenbezogenen Daten von Schülerinnen und Schülern auf *YouTube* ist untersagt, da sich sowohl der Sitz des Unternehmens als auch seine Server außerhalb des Geltungsbereichs der DSGVO – also der EU – befinden.

Medienpädagogische Einschätzung

Die Möglichkeit, Eigenproduktionen öffentlich zu machen, kann Schülerinnen und Schüler zusätzlich motivieren, mediengestalterisch aktiv zu werden. Daher sollte bei der Planung von größeren Medienprojekten die Präsentation bzw. Veröffentlichung der Ergebnisse gleich mitgedacht werden. Die restriktiven Verwaltungsvorschriften hinsichtlich der schulischen Nutzung von Nicht-EU-Plattformen sind aus datenschutzrechtlichen Gründen berechtigt. Auf der anderen Seite beschränken solche Verbote eine aktive Auseinandersetzung mit der kindlichen medialen Lebenswelt. Die Video-Plattform *YouTube*, auf der die meisten Kinder zumindest ab und zu Inhalte anderer konsumieren, könnte als gestaltbarer, öffentlich-medialer Raum erlebt werden, in dem eigene Anliegen ausgedrückt werden können. Dieser aktiv-produktive Zugang würde es auch erleichtern, kritische Aspekte der Plattform im Unterricht zu thematisieren, z.B. Hatespeech/Cybermobbing, (Schleich-)Werbung, Fake News, Traumberuf: *YouTuber/in*. Eine Veröffentlichung von medialen Schülerprodukten auf *YouTube* wäre aus datenschutzrechtlicher Perspektive nur möglich, wenn diese keine personenbezogenen Daten enthielten. Allerdings wären die Möglichkeiten des Selbstausdrucks der Kinder durch fehlende Körpersprache und verbale Äußerungen stark eingeschränkt. Auf Alternativen zu *YouTube*-Veröffentlichungen gehen wir im nächsten Beispiel ein.

Fallbeispiel 8:
Ein Schülervideo auf der Schulhomepage veröffentlichen

Situationsbeschreibung
Frau Müller möchte innerhalb einer Woche mit ihrer Klasse ein Märchen der Gebrüder Grimm verfilmen und das fertige Video, auf dem einzelne Kinder erkennbar sind, auf die Schulhomepage stellen. Der Film soll mit einem Schultablet gedreht und geschnitten werden.

Datenschutzrechtliche Aspekte	Erforderliche Maßnahmen
1  Video- und Stimmaufnahmen von Schülerinnen und Schülern sind **personenbezogene Daten**.	 Frau Müller benötigt **informierte Einwilligungen in Videoaufnahmen**. Kinder, deren Eltern nicht zustimmen, dürfen nicht gefilmt werden.
2  Die Klasse verwendet eine Woche lang ein **Schulgerät** (Tablet).	 Frau Müller reserviert ein Tablet für eine ganze Woche, um sicherzustellen, dass **keine dritten Personen Zugang zu den zwischengespeicherten Daten** erhalten. Nachdem sie das fertige Video auf dem Schulserver gespeichert hat, **setzt sie das verwendete Tablet zurück**.

Datenschutzrechtliche Aspekte	Erforderliche Maßnahmen
3  Frau Müller plant die **Veröffentlichung** des Videos auf der Schulhomepage.	 Frau Müller benötigt **informierte Einwilligungen in die Veröffentlichung von Videos auf der Schulhomepage**. Fehlt nur eine Einwilligung eines Elternteils, dessen Kind im Film erkennbar ist, veröffentlicht Frau Müller das Video nicht.

Medienpädagogische Einschätzung

Wie im vorhergehenden Beispiel erwähnt, kann die Aussicht auf die Veröffentlichung eines Projektergebnisses die Schülermotivation steigern. Sofern die betroffenen Sorgeberechtigten einverstanden sind, bietet die Schulhomepage unter datenschutzrechtlichen Gesichtspunkten einen sicheren Rahmen, da sie innerhalb der IT-Schulinfrastruktur gehostet – also betrieben – wird. Denkbar ist auch eine Veröffentlichung auf *Juki*, einer Videoplattform für Kinder, die in das Internetangebot *kindersache.de* des *Deutschen Kinderhilfswerks* eingebunden ist. Lehrkräfte können hier einen speziellen Schul-Account anlegen. Im Vergleich zur Schulhomepage ist dieses Angebot interessant, da es sich zum einen deutschlandweit an Kinder richtet. Zweitens bietet *Juki* die Möglichkeit, Videos zu kommentieren. Insbesondere Feedback anderer Kinder könnte sich sehr motivierend auf Schülerinnen und Schüler auswirken. Alle Kommentare werden vor der Freischaltung redaktionell geprüft. Bedenken Sie jedoch, dass die Zugriffszahlen von *Juki* nicht mit denen von *YouTube* vergleichbar sind. Zudem würde beim Upload eines Videos auf *Juki* eine Auftragsdatenverarbeitung vorliegen und die Schule müsste einen entsprechenden Vertrag mit dem *Deutschen Kinderhilfswerk* im Voraus abschließen.

Schließlich möchten wir Sie noch auf Fragen des Urheberrechts hinweisen. Bei der Veröffentlichung von Schülerarbeiten sollten Sie stets die Nutzungsrechte mit den Kindern selbst und ihren Eltern klären. Weitere Informationen zu Nutzungsrechten von Schülerarbeiten finden Sie auf dem Webportal der *Lehrerfortbildung Baden-Württemberg*.[27]

27 lehrerfortbildung-bw.de/st_recht/urheber/urh/nutz/minder

Fallbeispiel 9:
Nutzung eines Tablet-Koffers des Medienzentrums

Situationsbeschreibung
Im Rahmen einer Medienwoche entleiht die Schule einen Tablet-Koffer des Kreismedienzentrums. Frau Müllers Schülerinnen und Schüler sollen mit diesen Geräten einen Trickfilm erstellen und vertonen. Dabei können die Kinder ihre Stimmen aufnehmen und ein Portrait der eigenen Arbeitsgruppe in den Filmabspann einfügen.

Datenschutzrechtliche Aspekte	Erforderliche Maßnahmen
1  Foto- sowie Stimmaufnahmen von Schülerinnen und Schülern sind **personenbezogene Daten**.	 Frau Müller benötigt **informierte Einwilligungen in Foto- und Tonaufnahmen**. Kinder, deren Eltern nicht einwilligen, dürfen sich nicht fotografieren und auch keine Stimmaufnahmen machen.
2  Es handelt sich um **Leihgeräte**, die nach der Nutzung an das Medienzentrum zurückgehen.	 Bei der Ausleihe informiert sich Frau Müller beim Anbieter, über welche Schnittstelle erarbeitete Schülerprodukte (idealerweise im Schulnetz) gespeichert und wie die **Geräte vor der Rückgabe zurückgesetzt** und persönliche Schülerdaten gelöscht werden können.

Medienpädagogische Einschätzung
Trickfilm-Produktionen sind ein gutes Beispiel für *datensparsame*, kreativ-produktive Projekte. Sofern oben genannte Einwilligungen fehlen, können diese Kinder einfach auf sprachliche und fotografische Selbstaufnahmen verzichten, ohne einen Großteil des kreativen Spielraums zu verlieren.

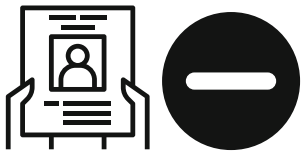
Des Weiteren beschäftigt sich dieses Fallbeispiel mit dem Angebot von Kreis- und Stadtmedienzentren. Ein Großteil der baden-württembergischen Grundschulen verfügt nicht über eigene Tablets. Leihgeräte der Medienzentren bieten daher eine niederschwellige und kostenlose Gelegenheit, um die ersten Erfahrungen mit mobilen Endgeräten im Unterricht zu sammeln. Ihre medienpädagogischen Beraterinnen und Berater können Projektideen liefern sowie Tipps zur technischen Bedienung und App-Empfehlungen geben. Darüber hinaus können Schulen über das Landesmedienzentrum Baden-Württemberg kostenlos erfahrene, medienpädagogische Referentinnen und Referenten beauftragen, ein Projekt gemeinsam mit einer Lehrkraft (Team-Teaching) durchzuführen.

Fallbeispiel 10:
Personenbezogene Daten in der Cloud speichern

Situationsbeschreibung

Frau Müller möchte ein persönliches digitales Klassenbuch führen, in dem sie den Leistungsstand ihrer Schülerinnen und Schüler, Stundenpläne, Schülerprojekte etc. dokumentieren und abrufen kann. Sie überlegt, hierfür einen Cloudspeicher zu nutzen, damit sie Daten sowohl mobil an ihrem Tablet als auch von zu Hause an ihrem PC eingeben und bearbeiten kann. Da auf dem Schulserver keine eigene Cloud betrieben wird, möchte Frau Müller den Service eines europäischen Anbieters nutzen.

Datenschutzrechtliche Aspekte	Erforderliche Maßnahmen
1  Namen, Benotungen, Beobachtungen etc. von Schülerinnen und Schülern sind **personenbezogene Daten**.	Frau Müller benötigt für die Verarbeitung dieser Daten keine informierten Einwilligungen der Eltern, da eine Rechtsgrundlage durch die Verwaltungsvorschriften des KM besteht.

Datenschutzrechtliche Aspekte	Erforderliche Maßnahmen
2  Frau Müller möchte das digitale Klassenbuch in den **Cloudspeicher** eines europäischen Anbieters stellen.	 Die Nutzung des Cloudspeichers eines externen Unternehmens verlangt immer einen **Vertrag zur Auftragsdatenverarbeitung** zwischen Schule und Unternehmen. Da dieser Schritt aufwändig und mit Unwägbarkeiten verbunden ist, empfehlen wir, **von einer externen Cloudlösung abzusehen**. Eine Alternative finden Sie in der folgenden Einschätzung.
3  Frau Müller möchte die Daten auf **privaten Geräten** (Tablet & PC) verarbeiten.	 Mit Hilfe eines **Antrags auf Nutzung privater Datenverarbeitungsgeräte für dienstliche Zwecke** holt Frau Müller die Zustimmung der Schulleitung ein. Frau Müller gewährleistet die **Sicherheit der Daten** auf ihren privaten Geräten, z.B. pseudonymisiert und verschlüsselt sie Schülerbewertungen auf ihrem PC. Von ihren privaten Geräten **löscht** Frau Müller **personenbezogene Daten** ihrer Schülerinnen und Schüler spätestens nach dem Ende des jeweils nächsten Schuljahrs.

Medienpädagogische Einschätzung
Neben einem verbesserten Lernen und Lehren können mit digitalen Medien administrative und organisatorische Aspekte effizienter gestaltet werden. Ein digital geführtes Klassenbuch erlaubt es, Schülerbewertungen und -beobachtungen, Schülerarbei-

ten, Unterrichtsplanungen etc. zentral zu dokumentieren und schnell abzurufen. Dadurch gewinnt die Lehrkraft potenziell Zeit für den Unterricht sowie für dessen Vor- und Nachbereitung. Allerdings muss bedacht werden, dass für die Einarbeitung in die neue Soft- und Hardware erst einmal Zeit investiert werden muss.
Zudem ist etwa die Aussage von digital dokumentierten Schülerbewertungen, die als Leistungsverläufe von bestimmten Apps grafisch dargestellt werden können, begrenzt. Wichtige Lernfaktoren, z.B. intrinsische Motivation, soziale Eingebundenheit in der Klasse, Lehrer-Schüler-Beziehung, klammern solche quantifizierten Darstellungen aus. Nichtsdestotrotz kann ein digital geführtes Klassenbuch durchaus einen großen Mehrwert haben. Für *iOS*, *MacOS* und *Windows* empfehlen wir die App *Meine Klassenmappe*, die speziell für den Grundschulbereich entwickelt wurde. Sie erlaubt eine datenschutzkonforme Speicherung und Synchronisation von Daten zwischen mobilen und stationären Geräten ohne Cloud-Lösung. Beachten Sie jedoch bitte, dass diese App keine Anhänge (z.B. Fotos, PDFs, MP3s) verschlüsseln kann.

6. Kapitel: Didaktische Materialien

Ein funktionierendes Datenschutzkonzept muss alle Akteure einer Grundschule berücksichtigen. Insbesondere Schülerinnen und Schüler müssen im Laufe dieses Prozesses angesprochen und mitgenommen werden. Denn sie sind es, deren personenbezogenen Daten verarbeitet werden bzw. sie verarbeiten auch selbst eigene und fremde personenbezogene Daten. Eine absolute Kontrolle dieser Datenverarbeitung ist weder möglich noch erstrebenswert. Beispielsweise ist es kaum zu verhindern, dass Schülerinnen und Schüler über Computerschnittstellen (z.B. USB, WLAN) oder durch das bloße Abfotografieren oder Abfilmen eines Bildschirms mit einem privaten Gerät sensible Daten eigenmächtig speichern. Eine Vereinbarung von komplexen Nutzungsordnungen für digitale Medien mag zwar juristisch wasserdicht sein, eine andere Frage ist jedoch, wie ein Kind in die Lage versetzt werden kann, diese Regelungen nachzuvollziehen und umzusetzen. Ein tragfähiges, schulisches Datenschutzkonzept sollte daher medienbildnerische Aspekte beinhalten.

Medienbildung setzt bei der Lebenswelt von Kindern an und soll sowohl ihre Alltags- als auch Medienerfahrungen aufgreifen. Daran anknüpfend eröffnet eine handlungsorientierte Medienbildung vielfältige Möglichkeiten, insbesondere unter Einbezug von digitalen Medien: Individualisierte und kooperative Lernprozesse, Informationsrecherche, Selbstausdruck und Kommunikation, Persönlichkeitsbildung, etc. Dabei sollen sowohl die positiven Potenziale digitaler Medien für Lernprozesse und Alltagshandeln als auch mögliche Risiken thematisiert und kritisch reflektiert werden.

Darüber hinaus ist Medienbildung als Leitperspektive seit dem Jahr 2016 verpflichtender Bestandteil des Bildungsplans des Landes Baden-Württemberg. Grundlage dieser Leitperspektive ist der Beschluss der Kultusministerkonferenz *Medienbildung in der Schule* aus dem Jahr 2012, in der eine schulische Medienbildung gefordert wird: *„Da Medienkompetenz weder durch familiale Erziehung noch durch Sozialisation oder die individuelle Nutzung von Medien in der Freizeit allein erworben werden kann, ist eine grundlegende, umfassende und systematische Medienbildung im Rahmen der schulischen Bildung erforderlich.“*[28] Die *Leitperspektive Medienbildung* soll fächerintegrativ und spiralcurricular in den Klassen 1-12 an allen allgemeinbildenden Schulen umgesetzt werden. Dabei sollen die Themen *Informationelle Selbstbestimmung* und *Datenschutz* in folgende sechs Bereiche der Medienbildung integriert werden: *Information und Wissen, Kommunikation und Kooperation, Produktion und Präsentation, Schützen und sicher agieren, Informationstechnische Grundlagen sowie Mediengesellschaft und -analyse*.[29]

---

28 kmk.org/fileadmin/veroeffentlichungen_beschluesse/2012/2012_03_08_Medienbildung.pdf

29 In der medienpädagogischen Fach-Community wird die *Leitperspektive Medienbildung* im Bereich der Grundschule durchaus kritisch gesehen. Horst Niesyto, emeritierter Medienpädagogik-Professor der PH Ludwigsburg bemängelt, dass darin „insbesondere persönlichkeitsbildende Dimensionen von Medien, die produktiv-gestalterische Nutzung von Medien und datenschutzrechtliche Aspekte [zu kurz] kommen [...].“

Im Jahr 2019 veröffentlichte das *Landesmedienzentrum Baden-Württemberg* das *e-Portfolio Medienbildung*[30], in dem Lehrkräfte sowie Schülerinnen und Schüler Arbeitsergebnisse dokumentieren können. Bestandteil dieser Plattform ist ein Kompetenzraster, in welchem die oben aufgeführten Bereiche aufgegriffen und in Teilkompetenzen spiralcurricular differenziert werden, u.a. für die 1./2. und die 3./4. Klassenstufe. Nach Fächern geordnet kann zu den einzelnen Teilkompetenzen auf Unterrichtsmaterialien über die *SESAM-Mediathek*[31] zugegriffen werden, darunter auch zu den Themen *Datenschutz und informationelle Selbstbestimmung für die Grundschule*. Darüberhinaus ist zu diesen Aspekten das Angebot im Internet weitaus größer. Im Folgenden möchten wir versuchen einen umfassenden Überblick über kostenlose didaktische Materialien für die Grundschule aus dem deutschsprachigen Raum zu geben.

Unterrichtsentwürfe

Landesmedienzentrum Baden-Württemberg: Wir werden Datenprofis 1 & 2
https://sesam.lmz-bw.de/mediathek?inp=token:datenprofis
Auf diese beiden – insgesamt neun Unterrichtsstunden umfassenden – Module kann in der *SESAM-Mediathek* zugegriffen werden. Die Module wenden sich an Kinder der 3. und 4. Klassenstufe und beinhalten detaillierte didaktische Hinweise, Unterrichtsverläufe, Lösungsblätter sowie Arbeitsmaterialien. Auch wenn die Unterrichtsszenarien überwiegend kognitiv beanspruchend sind und wenige Möglichkeiten für kreativen Selbstausdruck bieten, ist die gründliche Ausarbeitung sowie die Themen- und Methodenvielfalt positiv hervorzuheben.

Safer-Internet.at: Safer Internet in der Volksschule
https://www.saferinternet.at/fileadmin/categorized/Materialien/Safer_Internet_in_der_Volksschule.pdf
Die von der Europäischen Union gefördert Initiative *Safer-Internet.at* wird durch das *Österreichische Institut für angewandte Telekommunikation* umgesetzt. Der Leitfaden *Safer Internet in der Volksschule* – die vierjährige Volksschule in Österreich entspricht der deutschen Grundschule – umfasst eine Vielzahl an Themenbereichen insbesondere zum Jugendmedienschutz, darunter ein Arbeitsblatt mit didaktischen Hinweisen zum Thema *Welche Informationen man online veröffentlichen darf*. Im Zusammenhang mit Datenschutz ist auch die letzte Lektion *Was ist online?* interessant, in der die Themen *Internet der Dinge* und *Überwachung* behandelt werden.

BEE SECURE: Pädagogischer Leitfaden zur Informationssicherheit
https://www.bee-secure.lu/sites/default/files/publications/Leitfaden_V2_digitalversion.pdf
BEE SECURE ist eine gemeinsame Jugendmedienschutzinitiative mehrerer luxemburgischer Ministerien. Der umfassende pädagogische Leitfaden wendet sich an Grund-

30 eportfolio.lmz-bw.de
31 sesam.lmz-bw.de

schullehrende, wobei die Schulzyklen (*Cycles*) 2 und 3 der deutschen Grundschule entsprechen. Gelungen ist u.a. die spielerische Methode *Das Passwort-Spiel* und das bildorientierte Arbeitsmaterial zum Thema *Schütze deine Privatsphäre*.

Klicktipps.net: kinder.sicher.online!
https://www.klick-tipps.net/multiplikatoren/kinder-sicher-online
Klicktipps.net ist eine Initiative von *jugendschutz.net*, dem Kompetenzzentrum von Bund und Ländern für Jugendmedienschutz im Internet. *kinder.sicher.online!* ist eine Sammlung von videogestütztem Unterrichtsmaterial für die Grundschule ab der 2. Klasse. In Lektion 5 *Reden über Medienerfahrungen* werden die Bereiche *Daten schützen* und *Passwort* thematisiert. Neben zwei Videos werden ein paar didaktische Hinweise, Arbeitsmaterialien und weiterführende Links angeboten.

Klicksafe.de: Durchs Jahr mit Klicksafe
https://www.klicksafe.de/service/schule-und-unterricht/durchs-jahr-mit-klicksafe/
Klicksafe.de ist eine EU-Initiative, die in Deutschland von der *Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz* und der *Landesanstalt für Medien NRW* umgesetzt wird. Ihr Grundschulleitfaden *Durchs Jahr mit Klicksafe* zum Thema *Jugendmedienschutz* richtet sich an 2.-5. Klassen. In Lektion 7 *Recht am eigenen Bild* sollen die Kinder einen Regelleitfaden für das Veröffentlichen von Fotos, auf denen Andere abgebildet sind, erstellen. Dieser Regelleitfaden bietet eine gute Basis für persönliche Entscheidungen. Allerdings ist die Gestaltung der Methode sehr textlastig und daher nur für Schülerinnen und Schüler mit angemessenen Lesekompetenzen geeignet. Darüber hinaus ist das Zusatzprojekt *Clash of Cats* erwähnenswert, da es das Thema der *Preisgabe personenbezogener Daten im Zusammenhang mit Online-Spielen* spielerisch aufbereitet.

Caritas Stuttgart: DigiTales
https://medienbildung-stuttgart.de/ueber-digitales-gs/
Die *DigiTales-Box* für Grundschulen besteht aus 40 Modulen á 90 Minuten, deren Anspruch es ist, Medienkompetenz und Gewaltprävention an Grundschulen zu fördern. Zwei Module widmen sich den Themen *Datenschutz* und *Privatsphäre*. *DigiTales* ist jedoch nicht frei erhältlich, Schulen müssen sich bei der *Caritas Stuttgart* bewerben.

SIN – Studio im Netz: Projekt Watching You
https://www.studioimnetz.de/projekte/watchingyou/
Das *SIN – Studio im Netz* – ist eine seit 1996 bundesweit agierende medienpädagogische Facheinrichtung. Im Projekt *Watching You* werden Methoden und Materialien für Lehrkräfte sowie Erzieherinnen und Erzieher rund um das Thema Datenschutz entwickelt. Der Bereich *Big Data und Datenschutz – für Kinder erklärt* wurde gemeinsam mit Kindern gestaltet und entspricht nicht professionellen Standards. Hervorzuheben ist die Lektion *Dein Geheimnis*, in der zwei Methoden zum Thema *Öffentlich und privat* für den Vorschulbereich präsentiert werden. Diese könnten selbstverständlich auf Grundschulkinder der 1. und 2. Klasse angepasst werden.

Lern- und Übungsmaterial

Die Berliner Beauftragte für Datenschutz: Data-Kids.de
https://data-kids.de/
Data-Kids.de ist ein Internetportal der *Berliner Beauftragten für Datenschutz* für Lehrkräfte, pädagogische Fachkräfte, Eltern und Kinder. Für den Einsatz ab der 3. Klasse wird ein Lern- und Übungsbuch angeboten. Eingebettet in eine kleine Geschichte mit ansprechend illustrierten Charakteren sollen Grundbegriffe, wie z.B. Netzwerk, on/offline, Passwort, vermittelt werden. Die Materialien und Methoden sind didaktisch eher schlicht und textlastig gestaltet (z.B. Lückentexte, Begriffspaare bilden, Kreuzworträtsel). Positiv hervorzuheben ist das Kapitel 3, in dem Schadsoftware verständlich – auch mit Hilfe eines Videos – erklärt wird.

Internet-ABC e.V.: Lernmodul Datenschutz - das bleibt privat!
https://www.internet-abc.de/kinder/lernen-schule/lernmodule/datenschutz-das-bleibt-privat/
Hinter dem *Internet-ABC* stehen die Medienanstalten der Länder, u.a. auch die *Landesanstalt für Kommunikation (LFK) Baden-Württemberg*. Die Plattform bietet vielfältige Inhalte für Kinder, Eltern und Lehrkräfte, u.a. 15 Lernmodule aus den vier Themenbereichen *Surfen und Internet*, *Mitreden und Mitmachen*, *So schützt du dich* und *Medien im Internet*. Die Lernmodule bestehen jeweils aus mehreren Arbeitsblättern, die von Kindern der 3.-6. Klassen bearbeitet werden können. *Datenschutz - das bleibt privat!* ist eine der 15 Lektionen, die u.a. folgende Aspekte thematisiert: *Unterschied zwischen öffentlich und privat, Preisgabe persönlicher Daten, Schutzmöglichkeiten vor Datenmissbrauch*. Positiv hervorzuheben ist die Vertonung sämtlicher Texte in der Online-Version. Alle Materialien stehen auch zum Download bereit. Erwähnenswert ist zudem der pädagogische Leitfaden *Mein erstes Internet-ABC*, der sich an Schülerinnen und Schüler der ersten beiden Klassen richtet und u.a. auch ein Kapitel zum Thema *Privatsphäre* enthält.

Videoclips

Seitenstark e.V.: Charlie und das Geheimnis der Daten
https://www.seitenstark.de/kinder/internet/charlie-clips/charlie-und-das-geheimnis-der-daten
Dieses 3-minütige Video von *Seitenstark e.V.*, einem Netzwerk von Kinderseiten, ist ansprechend gestaltet und thematisiert insbesondere den Bereich der Preisgabe von personenbezogenen Daten. Der Filmclip kann heruntergeladen und somit auch offline vorgeführt werden. Didaktische Zusatzmaterialien liegen jedoch nicht vor.

Planet Schule: Elli Online
https://www.planet-schule.de/sf/filme-online.php?reihe=1403
In dieser Reihe von *Planet Schule*, dem Bildungsprojekt der Sendeanstalten *SWR* und *WDR*, erlebt *Elli Online* zusammen mit ihrer Computermaus *Cosmo* Abenteuer im Internet. Jede der sieben ca. 4-minütigen Folgen ist sehr ansprechend gestaltet und kann heruntergeladen werden. Dabei werden Jugendmedienschutzthemen, wie z.B. *Passwortsicherheit* und *Preisgabe personenbezogener Daten* behandelt. Nicht zu empfehlen ist jedoch die Folge über *Bilder im Netz*. Das Verschicken von Löschaufforderungen per Post ist wohl kaum eine geeignete Maßnahme, um Kinder aus der eigenen Klasse dazu zu veranlassen, peinliche Bilder von ihren Privatgeräten zu entfernen. Stattdessen sollte in solch einem Fall die Schule informiert werden.

motzgurke.tv: Wie viel darf man im Netz preisgeben?
https://www.kindernetz.de/infonetz/medien/netzwerke/daten/-/id=257758/nid=257758/did=257770/5omq93/index.html
In dieser 4-minütigen Folge von *motzgurke.tv* des *SWR* besucht die Kinderreporterin *Lina* ein Mitglied des *Chaos Computer Clubs* und erfährt von ihm wichtige Datenschutztipps zum Thema *Soziale Netzwerke*, insbesondere *Facebook*. Inhaltlich und gestalterisch ist diese Reportage gut gemacht, allerdings ist *Facebook* mittlerweile für (ältere) Grundschulkinder keine relevante Plattform mehr.

Web-Apps[32]

Internet-ABC e.V.: Surfschein
https://www.internet-abc.de/lehrkraefte/unterrichtsmaterialien/surfschein/
Der *Surfschein* auf dem Portal *Internet-ABC* ist ein ansprechend gestaltetes, multimediales Quiz, das in einer Lang- und einer Kurzfassung vorliegt. In beiden Versionen können einzelne oder Gruppen von Schülerinnen und Schülern gegeneinander antreten. Auf der *Themeninsel Achtung Gefahren!* gibt es auch einige datenschutzrelevante Fragen. Mittlerweile kann die Programmdatei des Quiz heruntergeladen werden und auf *PC* oder *Mac* internetunabhängig gespielt werden. Das Quiz kann als Abschluss einer Unterrichtsreihe durchgeführt werden, an deren Ende die Kinder einen *Surfschein* erhalten. Vorlagen können beim *Internet-ABC* bestellt werden.

Die Berliner Beauftragte für Datenschutz: Wolkig mit der Aussicht auf Datenlecks (Data-Kids.de)
https://data-kids.de/Spiele.html#gamebook
Dieses einfach gestaltete Quiz für Grundschülerinnen und Grundschüler thematisiert Fragen rund um das Thema *Datenschutz im Internet*. Zum Zeitpunkt der Veröffentlichung dieser Broschüre, war das Quiz sehr textlastig und enthielt nur wenige bildsprachliche Elemente.

32 Programme, die nicht lokal, sondern auf einem Server installiert sind. Auf Web-Apps wird über Browser zugegriffen.

Mecodia GmbH: Wie sicher ist mein Passwort?
https://checkdeinpasswort.de
Im Auftrag der *Landesinitiative Kindermedienland Baden-Württemberg* betreut die *Mecodia GmbH* die gestalterisch ansprechende Web-App *checkdeinpasswort.de*. Hier können Schülerinnen und Schüler Passwörter auf ihre Sicherheit testen. Dabei zeigt die App jeweils an, wie viel Zeit ein Hacker bräuchte, um das eingegebene Passwort zu knacken. Nach unseren Erfahrungen ist dieses didaktische Tool sehr anschaulich und motivierend für Kinder. Wichtig ist jedoch der Hinweis im Voraus, keine aktuellen Passwörter einzugeben. Ergänzt wird die Web-App mit einem umfassenden Leitfaden zu sicheren Passwörtern.

Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern: Netzwerkstar
http://www.netzwerkstar.de
Dieses Web-Quiz für 7- bis 10-jährige thematisiert unterschiedliche Aspekte des Datenschutzes. Dabei können die Spielerinnen und Spieler einen von zwei Avataren auswählen, den sie im Laufe des Spiels – sofern sie genug richtige Antworten erzielen – verändern können. Die Aufmachung des Quiz erinnert an Computerspiele der 80er-Jahre.

Infografiken

teachtoday: Datenquelle Nutzer
https://www.teachtoday.de/Informieren/Datenschutz/mediabase/pdf/Grafik_Datenquelle_Nutzer_3360.pdf
Die Infografik der *Telekom-Initiative teachtoday* ist eine inhaltlich und gestalterisch gelungene Zusammenfassung von Kategorien personenbezogener Daten und ihren typischen Quellen. Sie enthält zusätzlich zehn konkrete Verhaltenstipps zum Thema *Datenschutz*.

handysektor.de: Nutzungsbedingungen kurzgefasst
https://www.handysektor.de/mediathek/nutzungsbedingungen-kurzgefasst/
Die Jugendplattform *Handysektor.de* ist ein Gemeinschaftsprojekt der *Landesanstalt für Medien NRW* und des *Medienpädagogischen Forschungsverbundes Südwest*. Die drei Infografiken der Reihe *Nutzungsbedingungen kurz gefasst* sind ein gelungener und mutiger Versuch, die komplexen AGBs der Sozialen Medien *WhatsApp*, *Snapchat* und *Instagram* reduziert und übersichtlich darzustellen. Die Materialien eignen sich für ältere Grundschülerinnen und Grundschüler.

Kostenlose Schulveranstaltungen zum Thema Datenschutz

Die **Initiative Kindermedienland Baden-Württemberg** und der **Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.** bieten kostenlose Schüler-Workshops, Elternveranstaltungen und Lehrerfortbildungen rund um das Thema Datenschutz für Schulen in Baden-Württemberg an:

Initiative Kindermedienland Baden-Württemberg
https://101schulen.kindermedienland-bw.de/de/startseite/anmeldung/

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.
https://www.bvdnet.de/datenschutz-geht-zur-schule/

Anfragen können auch an die Ortsvereine (*Erfa-Kreise*) des **Chaos Computer Clubs e.V.** gestellt werden.
https://www.ccc.de/schule

7. Kapitel: Fazit und Ausblick

Digitale Medien, insbesondere mobile Endgeräte, haben – sofern sie pädagogisch sinnvoll eingesetzt werden – große Potenziale für das Lernen und Lehren in der Grundschule. Allerdings wirft ihr Einsatz auch neue Fragen auf: In gestalterisch orientierten Unterrichtsszenarien werden bestimmte personenbezogene Daten – z.B. Video-, Foto-, Sprachaufnahmen – erzeugt, für deren Verarbeitung keine Rechtsgrundlage besteht. Diese kann erst durch eine informierte Einwilligung der Sorgeberechtigten hergestellt werden, in der die Betroffenen über ihre Rechte aufgeklärt und die Bedingungen der Datenverarbeitung benannt werden.

Auch wenn die Schulleitung für den Datenschutz verantwortlich ist, so muss die einzelne Lehrkraft in der Praxis sicherstellen, dass diese Bedingungen eingehalten werden und den Betroffenen kein Schaden entsteht – etwa dadurch, dass Unbefugte Zugang zu personenbezogenen Daten bekommen. Hierzu führt die Lehrkraft eine Reihe technisch-organisatorischer Maßnahmen durch (z.B. Einrichtung von Zugangssperren, Verschlüsselung von Daten, Datenlöschung). Diese Abläufe sind im Idealfall in ein umfassendes Datenschutzkonzept der Schule eingebettet, das überhaupt erst ermöglicht, rechtlichen Ansprüchen der Betroffenen, z.B. Recht auf Auskunft, Widerruf und Datenlöschung, nachzukommen.

Teil dieses Konzepts sollten auch medienerzieherische Maßnahmen sein, die Schülerinnen und Schülern grundlegende Kompetenzen des Datenschutzes und der informationellen Selbstbestimmung vermitteln.

Wir hoffen, dass wir Ihnen – ungeachtet der dargestellten großen Herausforderungen und Unwägbarkeiten – alltagstaugliche Lösungswege näher bringen konnten. Selbst wenn Ihre Schule noch nicht über ein ausgearbeitetes Datenschutzkonzept verfügt, möchten wir Ihnen Mut zusprechen, Ihre ersten Schritte mit digitalen Medien im Unterricht zu machen.

Neue Methoden und Innovationen in der Schule bergen naturgemäß Ungeprüftes, Unausgereiftes, Lücken, das Risiko des Scheiterns. Pädagogische wie auch rechtliche Ziele können lediglich auf Idealzustände hin entwickelt werden, pädagogischer Erfolg bei allen Schülerinnen und Schülern ist ebenso unrealistisch wie *wasserdichte*, rechtliche Regelungen für alle denkbaren Konstellationen. Im tatsächlichen Einsatz von digitalen Medien verbleiben letztlich auch Fehler, Inkonsistenzen und Dilemmata. Es bleibt die Verantwortung jedes einzelnen Akteurs in einer Schule, selbstverantwortlich und im Team zu entscheiden, wie bestimmte Anforderungen konsequent angepackt werden können und wo bisweilen auch *Mut zur Lücke* angebracht ist.

Gleichzeitig stellen wir fest, dass Lehrkräfte spürbare Entlastungen für die Bewältigung datenschutzrechtlicher Anforderungen brauchen, um einen aktiv-produktiven Einsatz digitaler Medien zu befördern.

Dringend notwendig sind moderne IT-Strukturen an Grundschulen, welche eine effektive Verwaltung von Endgeräten und ein zentrales Dateiablagesystem ermöglichen, das Lehrkräften sowie Schülerinnen und Schülern gestattet – auch außerhalb der Schule – Dateien rechtskonform zu speichern und abzurufen, da kurz- und mittelfristig die Implementierung einer landesweiten Bildungsplattform nicht absehbar ist. Selbstverständlich sollen solche Strukturen nicht von Lehrkräften, sondern von IT-Spezialisten verwaltet werden. Entsprechende Stellen müssen für Fachpersonal geschaffen werden. Des Weiteren braucht es eine autorisierte Stelle (landes- oder bundesweit), die Apps für die Verwendung an Schulen zertifiziert. Statt Anwendungen rechtlich und technisch prüfen zu müssen, sollten Lehrkräfte ihre Ressourcen nutzen, um pädagogische Szenarien zu entwickeln. Hinsichtlich der elterlichen Einwilligung sollte geklärt werden, inwiefern die Einführung digital unterstützter Verfahren praxistauglich ist und für Entlastung sorgen kann. Zudem sollte geprüft werden, ob es rechtlich, ethisch und pädagogisch vertretbar ist, in den Landesgesetzen und Verwaltungsvorschriften eine Rechtsgrundlage zu schaffen, die es Schulen ermöglicht, Video-, Foto- und Sprachaufnahmen im Rahmen des Unterrichts unter weiterhin strengen datenschutzrechtlichen Auflagen zu verarbeiten.

Technische und rechtliche Rahmenbedingungen können sich jederzeit ändern. Daher möchten wir abschließend anregen, dass Lehrkräften auch zukünftig verständliche, befähigende Leitfäden – etwa durch das Kultusministerium und seine angeschlossenen Behörden – bereitgestellt werden, um das selbstbestimmte und eigenverantwortliche Arbeiten mit digitalen Medien in Schule und Unterricht zu befördern.

Weiterführende Links

Allgemeine Informationen zum Datenschutz

Datenschutz geht zur Schule: Pädagogischer Leitfaden für weiterführende Schulen mit anschaulicher Einführung für Lehrkräfte
https://www.bvdnet.de/datenschutz-geht-zur-schule/lehrerhandout/

Medienrechte für Kinder: Broschüre über Rechte im Umgang mit digitalen Medien
https://www.kindermedienland-bw.de/de/startseite/service/publikation/did/medienrechte-fuer-kinder/

FAQs zum Datenschutz an Schulen (Lehrerfortbildung Baden Württemberg)
https://lehrerfortbildung-bw.de/st_recht/daten/faq_ds/

Fortbildungen zu Datenschutz und Sicherheitsstrategien für PC und Internet für Lehrkräfte (Lehrerfortbildung BW)
https://lehrerfortbildung-bw.de/st_recht/daten/fb/lehr/index.html

Übertragung der Datenschutzerklärung der Homepage des Landes Baden-Württemberg in *Leichte Sprache*
https://www.baden-wuerttemberg.de/de/header-und-footer/datenschutz/datenschutz-in-leichter-sprache/

Zentrale Unterlagen des Kultusministeriums Baden-Württemberg

Informationen zum Datenschutz
https://it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit

Hinweise zum Einsatz mobiler Endgeräte (Stand März 2018)
https://it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/mobile

Leitfaden für die datenschutzkonforme Auswahl und Nutzung von Apps (Stand März 2018)
https://it.kultus-bw.de/site/pbs-bw-new/get/params_Dattachment/4695616/Handreichung-Auswahl-Apps.pdf

Netzbrief (Mai 2018)
https://it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/Netztechnik+_+Netzbrief

Informationen zur technischen Infrastruktur

Technische und konzeptionelle Überlegungen zum Tablet-Einsatz (Landesmedienzentrum Baden-Württemberg)
https://www.lmz-bw.de/netzwerkloesung/fachwissen/tablets-in-der-schule/
und
https://www.lmz-bw.de/fileadmin/user_upload/Downloads/Handouts/paedML_Dateien/paedML-Tablets-2019-06-19.pdf

Technische Bedienung von iPads

Videotutorialreihe “iPad Basiskurs” auf Youtube
https://www.youtube.com/watch?v=PKKigOCp7Hc&list=PLIsWHbp_ojlQelilJgbY-364h3ytu2lvTq

Autorenverzeichnis

Rymeš, Robert
Akademischer Mitarbeiter im Projekt dileg-SL, Abteilung Medienpädagogik,
Leiter des Arbeitskreises „Medienbildung in der Grundschule“,
Freier Medienpädagoge.
www.ph-ludwigsburg.de/17001.html und www.rymes.de,
eMail: robert@rymes.de, Twitter: @herrrymes

Walter, Roland
Diplom-Erziehungswissenschaftler und Fachinformatiker,
Mitarbeiter am Kreismedienzentrum Waiblingen.
eMail: r.walter@rems-murr-kreis.de

Iberer, Ulrich, Dr.
Akademischer Rat am Institut für Bildungsmanagement der Pädagogischen Hochschule Ludwigsburg,
Datenschutzbeauftragter der Pädagogischen Hochschule Ludwigsburg.
eMail: iberer@ph-ludwigsburg.de

Impressum

Datenschutz beim Einsatz digitaler Medien in der Grundschule –
Eine Handreichung für Lehrerinnen und Lehrer in Baden-Württemberg mit rechtlichen Grundlagen, pädagogischen Hinweisen und Fallbeispielen

Autoren: Robert Rymeš, Roland Walter, Ulrich Iberer

Herausgeber: Projekt „Digitales Lernen Grundschule Stuttgart/Ludwigsburg“ (dileg-SL), www.dileg-sl.de

Die Broschüre kann digital als PDF heruntergeladen werden unter:
www.dileg-sl.de/grundschule-datenschutz

Kontakt zur Bestellung der gedruckten Broschüre:
thorsten.junge@ph-ludwigsburg.de

Kooperationspartner: Unterstützt von der Landesanstalt für Kommunikation (LFK) Baden-Württemberg.

Diese Handreichung entstand im Rahmen des Projekts dileg-SL (Digitales Lernen Grundschule – Stuttgart/Ludwigsburg), welches die Deutsche Telekom Stiftung im Rahmen des Programms „Digitales Lernen Grundschule“ von 2016-2019 gefördert hat.

Zitationsvorschlag: Rymeš, Robert; Walter, Roland; Iberer, Ulrich (2019): Datenschutz beim Einsatz digitaler Medien in der Schule unter Berücksichtigung der rechtlichen Rahmenbedingungen in Baden-Württemberg. Handreichung für Schulleitungen, Lehrerinnen und Lehrer. Pädagogische Hochschule.
Online: http://www.dileg-sl.de/grundschule-datenschutz

Diese Broschüre steht unter der Creative Commons-Lizenz “Namensnennung” (by), d.h. sie kann unter Angabe der Autoren beliebig verändert, vervielfältigt, verbreitet und öffentlich wiedergegeben (z.B. online gestellt) werden. Der Lizenztext kann abgerufen werden unter: https://creativecommons.org/licenses/by/4.0/deed.de.

Titel-Foto: Projekt „Digitales Lernen Grundschule Stuttgart/Ludwigsburg“

Layout und Umschlaggestaltung: Marc Bodon, Stuttgart, www.bodon.de

Ludwigsburg, September 2019

Ziel dieser Handreichung ist wesentliche datenschutzrechtliche Vorgaben für den Unterricht mit digitalen Medien anhand von praktischen Fallbeispielen verständlich zu erklären, um Lehrerinnen und Lehrern – insbesondere jenen an baden-württembergischen Grundschulen – Mut zu machen, neue Technologien im Unterricht einzusetzen. Dabei werden neben der Darstellung der rechtlichen Aspekte auch pädagogische Hinweise gegeben. Diese Handreichung entstand im Rahmen des Projekts *dileg-SL (Digitales Lernen Grundschule – Stuttgart/ Ludwigsburg)*, welches die *Deutsche Telekom Stiftung* im Rahmen des Förderprogramms *Digitales Lernen Grundschule* von 2016-2019 gefördert hat.

dileg-SL

PH Ludwigsburg
University of Education

Deutsche
Telekom
Stiftung

LFK
Landesanstalt für Kommunikation
Baden-Württemberg