

UNTERRICHTEN MIT DIGITALEN MEDIEN

INFOBLATT – DATENSCHUTZ

Das Recht auf informationelle Selbstbestimmung ist ein Grundrecht. Persönliche Daten dürfen nur auf Basis gesetzlicher Bestimmungen oder wirksamer Einwilligungen der Betroffenen verarbeitet werden.

DATENSCHUTZ UND SCHULE

Der Datenschutz legt Regeln für die Verarbeitung von persönlichen Daten fest und schützt in der Schule das Selbstbestimmungsrecht von Schüler*innen und Lehrkräften. Schulen sind verpflichtet, nur in Übereinstimmung mit gesetzlichen Bestimmungen oder wirksamen Einwilligungen personenbezogene Daten zu verarbeiten "soweit dies zur Erfüllung des Unterrichts- und Erziehungsauftrages, der Schulplanung, der Schulorganisation sowie der Schulaufsicht" erforderlich ist (Artikel 1, Absatz 1, [SchulDSVO M-V](#)).

Was sind personenbezogene Daten?

Personenbezogene Daten sind Informationen, die direkt Rückschlüsse auf das Leben und die Persönlichkeit eines Menschen zulassen. Im Schulalltag werden solche Daten vielfach automatisiert und händisch, digital und analog verarbeitet, zum Beispiel in Form von:

- **Grunddaten** (Name, Anschrift, Geschlecht, Staatsangehörigkeit)
- **Leistungsdaten** (Noten, Zeugnisse, Prüfungsergebnisse)
- **Organisations- und Schullaufbahndaten** (Ausbildungsberufe, Abschlüsse, Entwicklungs- und Leistungsberichte)
- **sonstige Datenbestände** (Kurshefte, Notenlisten, Prüfungsakten)

Manche Informationen sind besonders schutzwürdig: Angaben etwa zur Religionszugehörigkeit, ethnischen Herkunft oder Gesundheit gehören dazu. Diese dürfen grundsätzlich nur mit ausdrücklicher Zustimmung der betroffenen Person verarbeitet werden.

Profitipp:

Für die Datenverarbeitung und -sicherheit sowie die Beachtung des Datenschutzes sind die Schulleitungen verantwortlich. Sie werden bei der Organisation von den gemeinsamen [Datenschutzbeauftragten](#) an Schulen des Zweckverbandes Elektronische Verwaltung in Mecklenburg-Vorpommern (eGo-MV) unterstützt.

Datenschutz als Unterrichtsthema

Die Förderung von Datenkompetenz unterstützt Schüler*innen sensibel und selbstbestimmt mit eigenen und fremden Daten umzugehen. Für die Thematisierung im Unterricht hält das [Projekt DigiBits](#) Inspiration und Unterrichtsmaterial bereit.



Rechtsgrundlagen für die Datenverarbeitung

Praxistipp:

Um Datensicherheit zu gewährleisten, haben Lehrer*innen unter anderem folgende Möglichkeiten:

- Pseudonymisierung (zum Beispiel statt Klarnamen)
- Verwendung von dienstlichen Mailadressen und verschlüsselter E-Mails
- Verschlüsselung von Festplatten, einzelnen Dateien, Ordnern und Datenträgern
- Verwendung starker Passwörter
- Einholung datenschutzrechtlicher Einverständniserklärungen

Mehr Tipps und Links finden Sie auf dem Infoblatt – Datensicherheit.

Take Away Botschaft:

Im digitalen Schulalltag müssen personenbezogene Daten (z.B. Kontaktdaten, Standortdaten, Schul- und Leistungsdaten usw.) von Schüler*innen, Erziehungsberechtigten und Lehrkräften geschützt werden. Dabei sind rechtliche Vorgaben aus der Schulgesetzgebung, dem Landes- und [Bundesdatenschutzgesetz](#) und der Europäischen Datenschutz-Grundverordnung ([DSGVO](#)) zu beachten.

UNTERRICHTEN MIT DIGITALEN MEDIEN

INFOBLATT – DATENSICHERHEIT

Datensicherheit im digitalen Schulalltag umfasst den Schutz von Nutzer*innendaten auf dem Server beziehungsweise in der Cloud, in digitalen Lernumgebungen und bei der Kommunikation zwischen Lehrkraft, Schüler*in und den Erziehungsberechtigten.

DATENSICHERHEIT IN DER SCHULE

Personenbezogene Daten sind im digital gestützten Unterricht vielfältigen Sicherheitsrisiken ausgesetzt. Um den Schutz der Daten zu gewährleisten, müssen Schulen als verantwortliche Stellen ein Verzeichnis von Verarbeitungstätigkeiten sowie ein Datenschutz- und Sicherheitskonzept erstellen, aktuell halten und umzusetzen (Artikel 6, Absatz 1, [SchulDSVO M-V](#)). Der unberechtigte Zugriff, der Missbrauch und der Verlust von sensiblen Daten kann bereits mit einfachen Maßnahmen verhindert werden:

Pseudonymisieren

Die Verwendung von Pseudonymen statt Klarnamen erschwert die Identifizierung. Hier ist wichtig, die pseudonymisierten Daten nicht mit Informationen zusammen zu speichern, die eine eindeutige Zuordnung erlauben.

→ Wie [Pseudonymisierung in der Praxis](#) geht, wird auf der Website [datenschutz-schule.info](#) erklärt.

Verschlüsseln

Festplatten, mobile Datenträger, einzelne Dateien und Ordner mit sensiblen Daten können durch Verschlüsselung vor Verlust und unberechtigten Zugriffen geschützt werden.

→ Praktische [Tipps zur Verschlüsselung](#) hat der Verein [Digitalcourage](#) zusammengefasst.

Vertraulich kommunizieren

Die Nutzung dienstlicher Mailadressen, verschlüsselter E-Mails und digitaler Signaturen schützt sensible Daten in der Kommunikation zwischen Lehrkraft und Schüler*in bzw. den Erziehungsberechtigten.

→ Konkrete [Handlungsempfehlungen für eine sichere E-Mail Kommunikation](#) werden auf der Website [datenschutz-schule.info](#) beschrieben.

Starke Passwörter verwenden

Der Einsatz komplexer Passwörter schützt vor unberechtigtem Zugang zu Endgeräten, digitalen Lernumgebungen oder Dateien und somit den Zugriff auf sensible Daten.

→ Worauf es bei [Erstellung sicherer Passwörter](#) ankommt, erklärt das Bundesamt für Sicherheit in der Informationstechnik (BSI).

**Sichern und Wiederherstellen**

Das regelmäßige Kopieren und Sichern von Daten auf verschlüsselten und durch ein Passwort gesicherten Datenträgern schützt vor Verlust und ermöglicht das Wiederherstellen von Daten.

→ Wie [nachhaltige Datensicherung](#) gelingt, beschreibt das Zentrum für Schulqualität und Lehrerbildung (ZSL) Baden-Württemberg.

Geräte schützen

Der Einsatz professioneller Firewalls und aktueller Virenschutzprogramme schützt Endgeräte und somit sensible Daten vor Gefahren aus dem Internet.

→ Was bei der [Einrichtung von Schutzprogrammen](#) beachtet werden muss, hat das Kultusministerium Baden-Württemberg zusammengefasst.

Datenschutzkonform agieren

Die Verwendung von Onlinetools und Apps, die den datenschutzrechtlichen Vorgaben der DSGVO folgen sowie die datensensible Nutzung ermöglichen, stärken den Datenschutz.

→ Wie [datenschutzkonforme Apps und Webanwendungen](#) ausgewählt und eingesetzt werden, erklärt das Projekt [DigiBits](#).

Sicher und datensparsam surfen

Einstellungen im Webbrowser helfen, anonymer durch das Internet zu surfen und Datenspuren zu minimieren.

→ Eine [Anleitung zum sicheren Surfen im Internet](#) stellt der Verein [Digitalcourage](#) zur Verfügung.

Take Away Botschaft:

Die eigenen Daten und die der Schüler*innen zu schützen, gehört zum zeitgemäßen Lernmanagement. Pseudonyme, starke Passwörter und Verschlüsselungen sind leicht umsetzbare Sicherheitsmaßnahmen.