Stand: 03/2018

Mobile Endgeräte im Unterricht

Schulleiterinnen und Schulleiter tragen nach der Europäischen Datenschutzgrundverordnung (EU-DSGVO) als Verantwortliche die Gesamtverantwortung für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten der Schülerinnen und Schüler sowie der Lehrkräfte an der betreffenden Schule. Darüber hinaus sind alle Lehrkräfte verpflichtet, in ihrem jeweiligen Tätigkeitsbereich die datenschutz- und urheberrechtlichen Vorschriften einzuhalten.

Eine Verarbeitung von Schüler-, Lehrer- und Elterndaten darf ohne Einwilligung der Betroffenen durch die Schule nur dann erfolgen, wenn es eine legitimierende Rechtsvorschrift, z. B. für die Erfüllung des Erziehungs- und Bildungsauftrags der Schule zulässt. Dabei ist wichtig, dass die Verarbeitung personenbezogener Daten zur Aufgabenerfüllung zwingend erforderlich ist, d. h. der Zweck, für den die Datenverarbeitung erfolgt, kann auf anderem Wege ohne die Verarbeitung personenbezogener Daten nicht erreicht werden.

Nachfolgend erhalten Sie Hinweise und Empfehlungen, wie bzw. mit welchen Anforderungen mobile Endgeräte wie Smartphones, Tablets, Notebooks, Laptops usw. (sog. „mobile devices“) im Rahmen u. a. der geltenden Datenschutzbestimmungen in die unterrichtliche Nutzung einbezogen werden können. Hierbei wird nur die Nutzung von schuleigenen Geräten betrachtet.

Muss beim Einsatz von mobilen Geräten ein Auftrag zur Datenverarbeitung erteilt werden?

Soweit personenbezogene Daten durch andere Personen oder Stellen außerhalb der Schule verarbeitet werden, liegt eine Auftragsverarbeitung personenbezogener Daten i. S. d. Art. 28 EU-DSGVO vor, dessen Voraussetzungen eingehalten werden müssen.
Die Dienstleistung wird hierbei durch eine andere Stelle oder Einrichtung erbracht. Dies kann z. B. die Nutzung der Dienste eines Rechenzentrums sein (beim Schulträger, in einem anderen Rechenzentrum oder auch bei Cloud-Diensteanbietern). Auch die Nutzung vieler webbasierter Technologien und die Durchführung von Wartungsarbeiten oder vergleichbarer Hilfstätigkeiten, also z. B. Hardwarewartung an Servern oder Festplattensystemen, Betreuung des Betriebssystems usw. gelten als Auftragsverarbeitung.

Den Auftrag zur Datenverarbeitung vergibt die Schulleitung. In diesen schriftlichen Auftrag sind mindestens folgende Punkte aufzunehmen:

- Gegenstand und Umfang der Datenverarbeitung: Es ist darzustellen, welche personenbezogenen Daten auf welche Weise zu welchem Zweck/mit welchem Ziel verarbeitet werden. Welche Software wird dazu eingesetzt?
- Etwaige Unterauftragsverhältnisse: Dabei ist zu regeln, ob Unterauftragsverhältnisse gewünscht bzw. zugelassen sind. Es wird empfohlen, dass eine Erteilung eines Unterauftrags nur nach vorheriger Zustimmung der Schule erfolgen darf.
- Verpflichtung des Dienstleisters zur Vertraulichkeit .
- Die zu treffenden technischen und organisatorischen Maßnahmen. Die Maßnahmen sind konkret und detailliert festzulegen.
- Datenschutz- und Sicherheitskonzept mit den vom Auftragnehmer zu treffenden Maßnahmen.
- Unterstützungspflicht des Dienstleisters bei der Umsetzung der Betroffenenrechte durch den Verantwortlichen.
- Lösch- oder Rückgabepflicht der Daten nach Anschluss der Verarbeitung.

Bei der Auswahl eines Anbieters bzw. Auftragnehmers im Sinne einer Auftragsdatenverarbeitung ist es auch geboten, einen Blick auf die Allgemeinen Geschäftsbedingungen (AGB) zu werfen. Oft haben Anbieter bzw. Auftragnehmer im Sinne einer Auftragsdatenverwaltung in ihren AGBs Klauseln, die es ermöglichen, dass diese Bestimmungen durch den Anbieter einseitig und ohne Einverständnis des Auftraggebers geändert werden können. Ferner eröffnen sich manche Anbieter die Möglichkeit, personenbezogene Daten zu Werbezecken zu nutzen und manchmal sogar an Dritte zu übermitteln. Dies entspricht nicht dem Rechtsgedanken der EU-DSGVO, weshalb ein solcher Anbieter/Auftragnehmer für die entsprechende Auftragsdatenverwaltung ungeeignet ist.
Auf der Seite www.it.kultus-bw.de sowie auf der Seite http://lehrerfortbildung-bw.de sind zum Thema "Auftragsdatenverarbeitung" ein Mustervertrag sowie Hinweise des Kultusministeriums eingestellt.

Dürfen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben hervorgehen, auf dem mobilen Gerät verarbeitet werden?

Da diese Daten besonders schutzwürdig sind, dürfen sie grundsätzlich nicht auf mobilen Endgeräten verarbeitet werden.

Solche Daten dürfen nur dann verarbeitet werden, wenn eine besondere Rechtsvorschrift dies vorsieht oder der Betroffene ausdrücklich, auf die Verarbeitung dieser Daten bezogen, eingewilligt hat.

Was bedeutet die sog. Providerhaftung?

Schulen haften grundsätzlich unter den allgemeinen gesetzlichen Bestimmungen für durch sie zur Nutzung bereit gehaltene eigene Informationen (z. B. auf der Schulhomepage). Bei dem Thema Providerhaftung geht es darum, inwieweit Provider für fremde Informationen strafrechtlich und haftungsrechtlich (Schadensersatz) verantwortlich sind.
Die Schule ist Access-Provider, wenn sie Schülerinnen und Schülern einen Zugang zum Internet vermittelt. Access-Provider haften gemäß § 8 Telemediengesetz nicht, wenn sie sich aus dem Datenfluss heraushalten (reine Durchleitung). Da aber die Schule im Rahmen ihres Erziehungs- und Bildungsauftrags eine Aufsichtspflicht innehat und ausübt, gilt diese Haftungsfreistellung für Schulen nicht. Auch wenn durch den Provider (z. B. BelWü) Filter gegen jugendgefährdende Inhalte eingesetzt werden, gilt dieses Haftungsprivileg nicht, da sich die Schule dann ebenfalls nicht aus dem Datenfluss heraushält.
Auch ist die Schule für die Inhalte, die von den Schülerinnen und Schülern ohne unterrichtlichen Bezug gespeichert werden, und für andere zur Verfügung gestellt werden, als Host-Provider nach den allgemeinen Gesetzen verantwortlich.

Ist die Schule Access- oder Hosting-Provider, ist sie allerdings nicht verpflichtet, die von ihr übermittelten oder gespeicherten Informationen anlassunabhängig permanent zu überwachen und nach evtl. Rechtsverstößen zu suchen. Derartige Maßnahmen sind erst zu veranlassen, wenn konkrete Anhaltspunkte für eine durch Schülerinnen und Schüler begangen Rechtsverletzung oder Missachtung der Regeln bestehen.

Was bedeutet die sog. Störerhaftung?

Beim Thema Störerhaftung stellt sich die Frage der Haftung der Schule, wenn Schülerinnen oder Schüler über deren Anschluss Rechtsverletzungen (z. B. Urheberrechtsverletzungen) begehen.
Als Störer kann in Anspruch genommen werden, wer in irgendeiner Weise ursächlich zur Verletzung des geschützten Rechts beiträgt und zugleich zumutbare Verhaltenspflichten verletzt. Haftungsansprüche können z. B. Unterlassungs-, Widerrufs- oder Beseitigungsansprüche sein.
Die Störerhaftung setzt die Verletzung von Prüfpflichten der Schule voraus.

Der Schule bzw. den aufsichtführenden Lehrkräften obliegen Hinweis- und Überwachungspflichten hinsichtlich der Nutzung des Anschlusses. Den Schülerinnen und Schülern müssen daher Regeln zur Nutzung des zur Verfügung gestellten Anschlusses (z. B. im Rahmen der Nutzungsordnung) vorgegeben werden. Eine Verpflichtung der Schule, die Nutzung des Internets durch die Schülerinnen und Schüler permanent zu überwachen, die mobilen Endgeräte laufend zu überprüfen oder den Zugang zum Internet zu sperren, besteht grundsätzlich nicht. Derartige Maßnahmen sind erst zu veranlassen, wenn konkrete Anhaltspunkte für eine durch Schülerinnen und Schüler begangene Rechtsverletzung oder Missachtung der Regeln bestehen. Für die Einhaltung der Hinweis- und Überwachungspflicht ist entscheidend, dass sich die Schülerinnen und Schüler durch Lehrkräfte beaufsichtigt fühlen. Werden Hinweis- und Überwachungspflichten durch Lehrkräfte verletzt und hierdurch Rechtsverletzungen begangen, haftet die Schule (bzw. das Land). Rückgriff gegenüber Lehrkräften kann nur bei Vorsatz oder grober Fahrlässigkeit genommen werden.

Darf eine Lehrkraft ein Foto auf einem Handy, bei dem sie den Verdacht hat, dass es sich um Kinder- oder Jugendpornografie handelt, anderen Personen zeigen, um den Verstoß zu verdeutlichen?

Die Verbreitung, der Erwerb und der Besitz kinder- und jugendpornografischer Schriften ist gem. §§ 184 b, 184 c Strafgesetzbuch (StGB) unter Strafe gestellt. Ebenso wird gem. § 184 d StGB das Zugänglichmachen pornografischer Inhalte mittels Rundfunk oder Telemedien sowie der Abruf kinder- und jugend-pornografischer Inhalte mittels Telemedien bestraft.
Bei einem konkreten Verdacht sollte daher das Gerät an die Polizei für weitere Ermittlungen übergeben werden.

Welche Punkte muss ich bei der Inbetriebnahme von mobilen Endgeräten beachten?

Eine Aktivierung / Inbetriebnahme des Geräts soll möglichst ohne Verwendung personenbezogener Daten von Schülerinnen und Schülern erfolgen (Anonymisierung). Pseudonyme können ebenfalls verwendet werden. In Anbetracht des Erziehungs- und Bildungsauftrags der Schule und der durch die Schule wahrzunehmenden Aufsichtspflicht ist es datenschutzrechtlich unschädlich, dass die Schule hierbei eine Referenzliste pflegt, aus der die Zuordnung der Geräte oder der verwendeten Pseudonyme zu den Schülerinnen und Schülern ersichtlich ist.
Allerdings ist sicherzustellen, dass es einem eventuell beauftragten Dienstleister (Stichwort Auftragsdatenverarbeitung) nicht möglich ist, Rückschlüsse auf die dahinter stehenden Personen zu ziehen.

Es dürfen keine "privaten Bezahldaten" hinterlegt werden, wie z. B. Kreditkartendaten oder Bankverbindungen etc..

Eine entsprechende Firewall sowie ein Virenschutz müssen vorhanden sein, wenn die Nutzung des Internets oder E-Mail-Empfang ermöglicht wird. Werden personenbezogene Daten per E-Mail versendet, so muss dies verschlüsselt erfolgen.
Es muss eine vollständige Löschung aller personenbezogenen Daten auf dem Gerät möglich sein, so dass eine Wiederherstellung (auch unter Zuhilfenahme einschlägiger Software) nicht möglich ist. Diese Löschung ist vor einer Weitergabe eines Geräts an andere Nutzer und bei einer Außerbetriebnahme vorzunehmen.

Was ist der Unterschied zwischen anonymisierten und pseudonymisierten Daten?

Werden Daten anonymisiert, indem sämtliche Informationen, die auf eine Person hindeuten, entfernt werden, so verlieren sie ihren Personenbezug. D. h. man kann von diesen aus keine Rückschlüsse auf eine bestimmte oder bestimmbare Person ziehen. Bei anonymisierten Daten handelt es sich dann nicht um personenbezogene Daten. Werden keine personenbezogenen Daten verarbeitet, so findet die EU-DSGVO und das LDSG auch keine Anwendung.
Bei pseudonymisierten Daten wird der Personenbezug durch ein Merkmal (z. B. eine Zahlenfolge oder durch einen Alias wie Mogli56…, Schneewittchen34 etc.) ersetzt. So ist es grundsätzlich möglich, Rückschlüsse auf eine bestimmte oder bestimmbare Person zu ziehen. Oft wird auch eine Referenzliste gepflegt, aus denen sich die Zuordnung der Pseudonyme zu bestimmten Personen ergibt. Pseudonymisierte Daten sind personenbezogene Daten, weshalb die EU-DSGVO und das LDSG Anwendung finden.

Welche Einstellungen sollten bei der Inbetriebnahme auf jeden Fall vorgenommen werden?

Um zu vermeiden, dass andere Benutzer des Geräts auf die Daten zugreifen können, die sie in die Formularfelder von Webseiten eingegeben haben, sollte die Funktion des Browsers, diese Daten zu speichern, deaktiviert werden. Sofern bei einer App eine Speicherung des Passworts zur Authentifizierung möglich ist, darf diese Funktion nicht genutzt werden.
Oft sind aus datenschutzrechtlicher Sicht unerwünschte Dienste - das sind Dienste, die eine Verarbeitung personenbezogener Daten durchführen, die zur Aufgabenerfüllung der Schule nicht erforderlich sind - bei einem Endgerät bereits vorinstalliert.

Sämtliche evtl. bereits vorhandenen Apps/Dienste, die nicht benötigt werden, sind zu entfernen bzw. zu deaktivieren (z. B. Apps zu Cloud-Angeboten wie Dateiablagen). Eine Datenübermittlung zu Werbezwecken ist unzulässig. Eine Backup-Funktion, bei der eine Datensicherung in die Cloud erfolgt, ist zu deaktivieren.
Grundsätzlich sollen personenbezogene Daten außerhalb des Geräts nur im schulischen Netz bzw. in der Schule auf dem Schulserver gespeichert werden. Greifen mehrere Nutzer auf die Datenablage zu, müssen die Daten gegen unberechtigten Zugriff geschützt sein.
Um die Daten, die bisher zumeist lokal auf Schulservern in der Schule gespeichert werden, dennoch zentralisiert und über das Internet zugreifbar anbieten zu können, empfiehlt sich für die Umsetzung dieser zentralen Datenablage eine private Cloud, die ebenfalls datenschutzrechtskonform eingerichtet werden muss. Hinweise hierzu finden Sie auf it.kultus.bw zu "Cloud-Dienste im schulischen Bereich".
Geo- und Ortungsdienste (GPS und Funkzelleninformation) sind immer dann zu deaktivieren, wenn sie nicht für den Unterricht oder zu Kontrollzwecken benötigt werden. Eine Tracking-App zum Auffinden eines verloren gegangenen Geräts kann sinnvoll sein (Freigabe durch den Administrator). Geodaten dürfen nicht an Dritte übermittelt werden.

Welche Apps können verwendet werden?

Beim Bezug von Apps oder deren Updates ist darauf zu achten, welche Daten eine App verwenden will. So sind Zugriffsberechtigungen von Apps auf Kontaktdaten, die ohne Erforderlichkeit Zugriff auf die Kontaktdaten wünschen, zu deaktivieren.
Es sollen nur die unbedingt zur Gestaltung des Unterrichts notwendigen Apps installiert werden.
Kontakte, die personenbezogene Daten enthalten, dürfen nur im Rahmen des Auftrags der Lehrkraft und nur zu schulischen Zwecken angelegt werden.
Generell ist es ratsam, die Nutzung von Apps mit App- oder betriebssystemspezifischen Einschränkungen so zu konfigurieren, dass ein angemessener Kompromiss zwischen Benutzerfreundlichkeit und Datensparsamkeit getroffen wird. Um solche Einschränkungen technisch zentral umzusetzen, können Administratoren zum Beispiel Mobile-Device-Management-Systeme (MDM) einsetzen.
Einen Leitfaden für die datenschutzkonforme Auswahl und Nutzung von Apps finden sie auf dieser Homepage.

Was ist zu beachten, wenn die Foto-, Audio- und Videofunktionen benutzt werden?

Die Foto-, Audio- und Videofunktionalität darf nur dann im Unterricht genutzt werden, wenn folgende Rahmenbedingungen eingehalten werden:

- Fotos, Videos und Audioaufnahmen, auf denen Personen zu sehen bzw. zu hören sind, dürfen nur mit Erlaubnis der Lehrkraft sowie mit Einwilligung der Betroffenen gemacht werden.
- Die Aufnahmen dürfen nur zu unterrichtlichen Zwecken genutzt werden. Die Aufnahmen sind nach Abschluss des Arbeitsauftrages, spätestens jedoch am Ende des Schuljahres bzw. am Ende der Kursstufe zu löschen.
- Aufnahmen, die zu unterrichtlichen Zwecken gemacht wurden, dürfen grundsätzlich nicht Dritten gezeigt, an Dritte weitergegeben oder im Internet veröffentlicht werden, es sei denn, es liegen die schriftlichen Einwilligungen aller betroffenen Personen bzw. deren Erziehungsberechtigten entsprechend vor.
- Auf den Aufnahmen gezeigtes Verhalten von Schülerinnen und Schülern (z. B. Bewegungsabläufe beim Sport, aufgenommene Präsentationstechniken etc.) darf nicht unmittelbar zur Notengebung herangezogen werden. Dass Videoaufnahmen mittelbar zur Leistungsfeststellung beitragen, da sie als pädagogisches Mittel Einfluss auf die Leistung haben können und z. B. evtl. zur Leistungsverbesserung dienen, ist unschädlich. Möglich sind daher zum Beispiel Aufnahmen im Sportunterricht zur Vermittlung von Techniken oder im Kernfach Sport im Rahmen des Bewegungslehreunterrichts zur Bewegungsanalyse im Rahmen der in der Handreichung dargestellten Kriterien oder die Bewertung von Videos, die von Schülerinnen und Schülern zur Ergebnissicherung im Unterricht angefertigt wurden und bei der Lehrkraft eingereicht wurden, wobei nicht die Aufnahme des Verhaltens der Schülerinnen und Schüler Grundlage der Leistungsfeststellung sein darf.
- Unterrichtsmitschnitte (Audio und Video) dürfen nur im Auftrag der Lehrkraft und mit entsprechender Einwilligung der Betroffenen erfolgen.

Müssen für jede einzelne Foto-, Video- bzw. Audioaufnahme Einwilligungen eingeholt werden?

Es genügt, wenn zu Beginn des Schuljahrs, in dem Foto-, Video- bzw. Audioaufnahmen angefertigt werden sollen, bzw. bei der Anmeldung der Schülerinnen und Schüler eine entsprechende Einwilligung eingeholt wird. Die Einwilligung gilt bis zum Ende des Schulbesuchs. Mit Vollendung des 16. Lebensjahrs haben Schülerinnen und Schüler die nötige Einsichtsfähigkeit und müssen selbst einwilligen.
Soweit Foto-, Video- bzw. Audioaufnahmen veröffentlicht werden sollen, ist ab Vollendung des 14. Lebensjahrs zusätzlich zur Einwilligung der Erziehungsberechtigten auch die Unterschrift des/der betreffenden Schülers/Schülerin einzuholen.

In der Einwilligung ist gesondert anzugeben, für welche Zwecke und mit welchen Apps Aufnahmen angefertigt werden. Auch muss es der betroffenen Person möglich sein, deren Einwilligung auf einzelne Aufnahmezwecke zu beschränken (z. B. Videoaufnahmen im Rahmen eines Theaterstücks - ja, Videoaufnahmen im Rahmen des Sportunterrichts - nein).

Müssen personenbezogene Daten verschlüsselt werden?

Ja, werden personenbezogene Daten z. B. per E-Mail versendet, so muss dies verschlüsselt erfolgen. Speichert eine App personenbezogene Daten auf einem mobilen Endgerät, dann müssen die Daten verschlüsselt werden. Die Verschlüsselung kann bereits durch das Betriebssystem des Gerätes erfolgen. Ggf. muss die Verschlüsselung über die Konfiguration der App sichergestellt werden. Eine unverschlüsselte Speicherung personenbezogener Daten auf dem mobilen Endgerät ist datenschutzrechtlich unzulässig.

Was muss bei der Integration von mobilen Geräten in die schulische Infrastruktur beachtet werden?

Zur Anmeldung an die schulische Infrastruktur sind nur sichere Kennwörter zu verwenden. Entsprechende Empfehlungen sind auf der Homepage des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und auf dem Lehrerfortbildungsserver zu finden.
Es sind Vorkehrungen zu treffen, dass einmal gesetzte Sicherheitseinstellungen (Verschlüsselung, Virenschutz, Erzwingen von Passwörtern usw.) nicht durch die Schülerin bzw. den Schüler wieder umgangen werden können, z. B. per Mobile Device Mangagement (MDM).
Der Betrieb des Geräts muss ohne Administratorenrechte möglich sein (Apps werden stattdessen ggf. mit MDM ausgebracht s. o.). Jailbreaken oder Rooten (Eingriff in das Betriebssystem zur Erlangung maximaler Administratorenrechte) sollte - wenn dies möglich ist - technisch unterbunden werden.
Für den Zugang zu allen technischen Systemen in den Schulen, auch über WLAN, müssen die Nutzerinnen und Nutzer sicher identifiziert werden. Die zentrale Zielsetzung für die Authentifizierung besteht darin, jeder Nutzerin und jedem Nutzer eine eindeutige Benutzerkennung zur Verfügung zu stellen (Identity-Management), mit der diese über einen einzigen Anmeldevorgang Zugang zu allen ihnen zugeordneten und legitimierten Applikationen, Inhalten und Daten erhalten können (Access-Management). Dies betrifft sowohl Angebote, die von der Schule/den Schulträgern

selbst bereitgestellt werden, als auch den Zugriff auf Angebote von Drittanbietern. Im Idealfall erfolgt dies über eine einzige Anmeldung (Single Sign On).
Soweit für die Einrichtung bzw. zur Inbetriebnahme des mobilen Endgeräts individuelle E-Mail-Adressen nötig sind, sollten - wenn möglich - anonymisierte Klassen-E-Mail-Adressen verwendet werden. Im Übrigen sind die Vorgaben zum Thema "E-Mail im Unterricht" auf dem Lehrerfortbildungsserver zu beachten.
Im Übrigen sind gemäß Art. 32 EU-DSGVO durch die Schule als Verantwortlichen technische und organisatorische Maßnahmen zu treffen, die die Sicherheit der Daten gewährleisten. Technische Vorkehrungen zur Datensicherung sind z. B. der Einsatz von Filtersystemen oder die Protokollierung des Datenverkehrs.

Was ist zu beachten, wenn die Schülerinnen und Schüler das Gerät mit nach Hause nehmen dürfen?

Sollte die Schule ein Nutzungsrecht für die IuK-Technik außerhalb des Unterrichts z. B. für Hausaufgaben gewähren, so sind bei der Integration z. B. in das heimische WLAN die zuvor genannten Aspekte zu beachten. Daneben ist durch entsprechende Sicherungsmaßnahmen sicherzustellen, dass keine unbefugten Dritte auf personenbezogene Daten zugreifen können (z. B. dass nicht über Freigaben oder Berechtigungen über das WLAN auf personenbezogene Daten auf dem mobilen Endgerät zugegriffen werden kann). Virenschutz und Firewall sind zwingend erforderlich.

Was ist bei der Nutzungsordnung generell zu beachten?

Wer bei den einzelnen Regelungen für die Schule handelt, ist von der Schulleitung festzulegen und schulintern bekannt zu machen.
Die Regelungen für die Nutzung des Internets im Unterricht und außerhalb des Unterrichts zu unterrichtlichen Zwecken sind auch ohne Zustimmung der Schülerinnen und Schüler bzw. ihrer Sorgeberechtigten sowie der Lehrkräfte verbindlich. Die Nutzungsordnung muss aber eindeutig gestaltet und den Schülerinnen und Schülern sowie den Lehrkräften bekannt sein. Sie sollte als Teil der Hausordnung gut sichtbar in den Räumen der Schule, in denen eine Nutzung des Internets möglich ist, angebracht werden. Insbesondere sollte sie auch an dem Ort, an dem Bekanntmachungen der Schule üblicherweise erfolgen, angebracht werden. Ihre Einhaltung ist durch ausreichend häufige Kontrollen zu überprüfen.
Auch ist es möglich, eine bereits für die Nutzung schulischer Geräte im Netz existente Nutzungsordnung um eine Nutzungsordnung für schuleigene mobile Endgeräte zu erweitern.

Die Schülerinnen und Schüler bzw. deren Erziehungsberechtigte bestätigen mit ihrer Unterschrift, dass sie sich zur Einhaltung der Regelungen der (ggf. erweiterten) Nutzungsordnung verpflichten. Die Schülerinnen und Schüler sollten zu Beginn der schulischen Nutzung über die Nutzungsordnung belehrt werden. Diese Belehrung sollte im Schultagebuch protokolliert und jedes Jahr, zu Beginn des Schuljahres, wiederholt werden.
Die Schülerinnen und Schüler versichern durch ihre Unterschrift, dass sie die Nutzungsordnung anerkennen.

Verstöße der Schülerinnen und Schüler gegen die Nutzungsordnung können geahndet werden wie Verstöße gegen die Hausordnung der Schule bzw. gegen die Schulordnung und können pädagogische Erziehungsmaßnahmen nach sich ziehen.

Das Muster einer Nutzungsordnung für Schülerinnen und Schüler finden Sie auf dieser Homepage.

Wie sollte die Nutzungsordnung für die Nutzung der mobilen Geräte gestaltet sein?

Eine Nutzungsordnung muss insbesondere Aussagen zu folgenden Punkten enthalten:

- Nutzung des Schulnetzes im Unterricht,
- Einsatz des Internets im Unterricht und außerhalb des Unterrichts zu unterrichtlichen Zwecken,
- Zulässigkeit der Nutzung des Schulnetzes und des Internets außerhalb des Unterrichts in der Klasse oder im Kurs im Rahmen der medienpädagogischen Erziehung,
- Pflichten und Befugnisse der Schulleitung, des Systemadministrators, des Webmasters, der aufsichtführenden Personen, der Lehrkräfte sowie der sonstigen Nutzerinnen und Nutzer (insbesondere Art und Durchführung von Kontrollen),
- Hinweis auf die begrenzte Verantwortlichkeit der Schule für den Inhalt der über ihren Internet-Zugang abgerufenen Informationen,
- Verbot der Kommunikation von bestimmten Inhalten (wie fremdenfeindliche oder pornographische Inhalte) und von bestimmten Nutzungszwecken (wie zu gewerblichen oder allgemeinpolitischen Zwecken),
- Zulässigkeit, Umfang und Löschfristen der Aufzeichnung von Verbindungsdaten durch die Schule zu Kontrollzwecken (Aus Gründen der Aufsichtspflicht ist es zulässig, bei Internetzugriffen im Unterricht oder bei Internetzugriffen außerhalb des Unterrichts zu unterrichtlichen/ dienstlichen Zwecken automatisierte personenbezogene Protokolldateien zu führen.),

- Art und Durchführung von Kontrollen,
- Hinweis auf die Beachtung von Rechten Dritter (Urheberrechte usw.),
- Zuteilung und Verwaltung von Passwörtern,
- Sanktionen bei Verstößen gegen die Nutzungsordnung,
- Installation von Apps,
- Änderung der Systemkonfiguration einschließlich Sicherheitseinstellungen,
- Umgang mit personenbezogenen Daten (Löschfristen, Einwilligung etc.),
- Verbot von „rooten“ oder „jailbreaken“,
- Zulässigkeit von Private Browsing (Es ist zwar datenschutzrechtlich zulässig, dass die Lehrkraft Private Browsing zulässt oder anordnet, jedoch wird aus Gründen der Aufsichtspflicht empfohlen, auf Private Browsing zu verzichten.).