Datenschutz in der Schule und zu Hause

Ein kurzer Überblick für Lehrkräfte

Grundlagen

Datenschutz im Unterricht

Datenschutz im Kontakt zu Eltern und Außenstehenden

Datenschutz bei Nutzung der privaten IT-Ausstattung für dienstliche Zwecke

Stand des Entwurfs: 02.10.2018

Datenschutzbeauftragter für das Schulamt Weißenburg-Gunzenhausen:

Herr Stefan Schaller, Stephani-Mittelschule, Hindenburgplatz. 2, 91710 Gunzenhausen

datenschutzbeauftragter@schulamt-wug.de

1. Überblick Datenschutz

1.1. **Grundlagen** für alle Inhalte sind das BayEuG und das Bayerische Datenschutzgesetz sowie die DS-GVO. Einen Überblick liefert auch das aktualisierte Schulleiter-ABC. Eine Übersicht zu häufig gestellten Fragen finden Sie auch unter: https://lehrerfortbildung-bw.de/st_recht/daten/faq_ds/ (Beachten Sie aber die Ausführungen für Bayern seitens KM und des Landesbeauftragen

1.2. Personenbezogene Daten:

Personenbezogene Daten sind Einzelangaben über:

- ❖ persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen (Betroffene)
- ❖ *Bsp.: Name, Adresse, Alter, Religion, Krankheiten, Behinderungen, Förderempfehlungen, Leistungen, Besitz, aber auch Nutzungsdauer und –art, besuchte Internetseiten, Fotos, Ton- und Filmaufnahmen…*

Laut BayEuG Art. 85 dürfen folgende personenbezogene Daten im Schulbetrieb erfasst werden:

- **Schüler:** Name, Adressdaten, Staatsangehörigkeit, Religionszugehörigkeit, Migrationshintergrund, Leistungsdaten, Daten zur schulischen und beruflichen Vorbildung sowie zur Berufsausbildung
- **Lehrkräfte:** Name, Staatsangehörigkeit, Adressdaten, Angaben zur Lehrbefähigung und zum Unterrichtseinsatz, Beurteilungen
- **Erziehungsberechtigte:** Name und Adressdaten

2. Datenschutz in der Schule

2.1. Schülerakten und Klassentagebücher

- Schülerakten verlassen nicht die Schule. Sollten die Kollegen die Schülerakten selber führen, bzw. regelmäßig darin arbeiten (Zeugnisse abheften o.ä.), sollte diese Tätigkeit zeitlich und räumlich festgelegt werden.
- Der datenschutzrelevante Teil des Klassenbuches, also Schülerliste, (Ordnungsmaßnahmen, Fehlzeiten, Leistungsdaten etc.) ist im Klassenraum bzw. in einem anderen Raum der Schule aufzubewahren. Ein Verschluss ist notwendig, wenn Schüler alleine in der Klasse sind bzw. andere Personen das Klassenzimmer betreten können (Reinigungspersonal, Reparaturen finden statt, etc.). Ansonsten ist es so auszulegen, dass die in der Klasse unterrichtenden Kollegen damit arbeiten können.

2.2. Im Klassenzimmer

- Werden im Klassenzimmer IT-Systeme (PC, Notebook, Tablet-PC, Pads, etc.) verwendet, müssen die auf diesen eingesetzten Programme im behördlichen Verfahrensverzeichnis erfasst werden, sobald datenschutzrelevante Daten (digital) verarbeitet werden. Seit 2012 regelt zudem die „Nutzungsordnung für EDV-Einrichtung und Internet“ den Einsatz der IT-Systeme.
- Eine öffentliche Bekanntgabe (Vorlesen im Klassenverband) der Noten soll unterlassen werden.
- Eine öffentliche Bekanntgabe von Ordnungsmaßnahmen ist verboten. Die Androhung darf öffentlich ausgesprochen werden.
- Listen mit persönlichen Daten, z.B. sogenannte Notfalllisten, sollten in einem geschlossenen Umschlag aufbewahrt werden.
- Fotositzpläne sollen vermeiden werden. Generell soll mit dem Anfertigen von Schülerfotos äußerst sparsam umgegangen werden (vgl. Landesbeauftragter 02.07.2018)
  Beachten Sie: Bei Fotos, auch für unterrichtliche Zwecke, muss immer die Einverständniserklärung der Eltern vorliegen. Die Freigabe zu Jahresbeginn (KMS 2012) deckt nicht alles ab! Bitte informieren Sie die Eltern immer bei größeren Vorhaben **anlassbezogen** (verwenden Sie ggf. die Mustervorlage).
- Aushänge mit negativen Merkmalen (soziale Pranger) z.B. vergessene Hausaufgaben, Verhalten im Unterricht sind kritisch zu sehen. Vermeiden Sie immer Klarnamen und setzten Sie diese zumindest am Ende des Unterrichtstages auf „Null“ zurück. Bedenken Sie, dass am Nachmittag ggf. das Reinigungspersonal diesen sehen kann.

2.3. PC-Räume/Schüler PCs

- Achten auf die Geheimhaltung des Passworts für den Lehrerzugang am Computer
- In PC-Räumen muss es eine Nutzungsordnung geben, die von Lehrern und Schülern unterschrieben wird.
- Achten Sie auf die Löschfristen wenn Sie Daten im Schulnetzwerk ablegen.
- Achten Sie auf die Zugriffsrechte, wenn Sie Daten für alle zur Verfügung stellen (z.B. gute Schülerarbeiten -> pseudonymisieren).
- Computer müssen geschützt sein und der Schutz sollte regelmäßig überprüft werden (Virenscanner, Firewall-…).
- Fragen Sie immer beim Systembetreuer nach, wenn Ihnen etwas unklar ist bzw. Sie Datenschutzverletzungen erkennen.

2.4. Lernplattformen und Internet-Angebote

Folgende Überlegungen sollten Sie bedenken:

- Welche Daten erhält der Anbieter? Greift der Datenschutz bzw. sind es überhaupt datenschutzrelevante schulische Daten?
- Wo werden die Daten gehostet? (Keine Dropbox und kein WhatsApp für datenschutzrelevante dienstliche Daten!)

- Freigabe des Verfahrens muss vorhanden sein.
- Verwenden Sie sichere Passwörter und ggf. eine Pseudonymisierung
- Die Nutzung einer Lernplattform ist freiwillig und setzt die Einwilligung der Betroffenen (Lehrkräfte und Schüler) voraus. Eine Nichtteilnahme darf kein Nachteil sein.
- Der Einsatz einer Lernplattform (z.B. MEBIS) kann zum verpflichtenden Bestandteil des Unterrichts erklärt werden.
- Schulwebseite und Veröffentlichungen
  - Schriftliche Einverständniserklärung muss vorliegen (ab 14 Jahre auch vom Jugendlichen selbst).
  - Dies sollte als Standardformular (Vorlage KM 2012) von der Schule festgelegt und zum Schuljahresbeginn ausgefüllt werden. Ein Widerruf ist dabei jederzeit möglich. Beachten Sie dabei immer die Vorgaben der DS-GVO.

2.5. Wettbewerbe

- Wägen Sie die Kosten und den Nutzen im pädagogischen Kontext ab.
- Personenbezogene Daten dürfen nur mit Einverständniserklärung der Eltern (und ab 14 auch der Schüler) übermittelt werden
- Eine inhaltliche Prüfung der Angebote ist im Vorfeld vom Lehrer durchzuführen.
- Die übermittelten Daten sollten ggf. im Verfahrensverzeichnis erfasst werden.
- Es haftet auch hier der Leiter der Behörde.

3. Datenschutz im Kontakt zu Eltern und Außenstehenden

Grundsätzlich dürfen personenbezogene Daten **nur an Berechtigte** weitergegeben werden **(Verschwiegenheitspflicht)**. Dies gilt sowohl für digitale als auch analoge Weitergabe!

3.1. Eltern

- Beachten Sie: Gerade bei den sogenannten Tür- und Angel-Gesprächen vergisst man gerne, dass man über sensible Themen spricht. In solchen Fällen hören nicht selten auch andere (Kinder, Eltern) zu.
- Zur Erinnerung: In Elterngesprächen nur über das „eigene" Kind sprechen. Bei der Thematisierung von Problemen oder Vorkommnissen in der Klasse **keine anderen Kinder namentlich** nennen.
- Idee: Um zu gewährleisten, dass bei Ausflügen oder auch bei Elternbeteiligung im Unterricht keine Informationen über andere Kinder nach außen getragen werden, könnte man eine Verschwiegenheitserklärung unterschreiben lassen.
- Bei E-Mailkontakt ist zu beachten, dass keine sensiblen Daten übermittelt werden. Dies gilt besonders für nichteuropäische E-Mail Konten (z.B. G-Mail). Auch eine Verschlüsselung ist hier nicht zulässig. Führen Sie lieber ein persönliches Gespräch oder nutzen Sie den Postweg über die schulische Verwaltung.
- Eine Weitergabe von personenbezogenen Daten über WhatsApp ist nicht zulässig!

3.1. Außenstehende

- „Die Schülerdaten dürfen Dritten nicht zugänglich gemacht werden;…; die Regelung zum Datengeheimnis bzw. der Verschwiegenheitspflicht von Beamten ist zu beachten". **Dritte sind auch Ehepartner, Kinder, Freunde der Lehrkraft**.
- Auch bei Gesprächen mit schulnahen Institutionen wie z.B. Erziehungsberatung: Zuhören ist erlaubt - nachfragen nicht!
- Beachten Sie immer Ihre dienstrechtlichen Vorgabe und Fragen Sie bei der Schulleitung oder Ihrem Datenschutzbeauftragen nach.

4. Datenschutz zu Hause

Grundsätzlich müssen Sie auch zuhause den Datenschutz einhalten, wenn sie personenbezogene Daten verarbeiten wollen. Dies gilt sowohl in digitaler als auch analoger Form.

- Personenbezogene Daten von Schülerinnen und Schülern auf privaten Datenverarbeitungsgeräten der Lehrkräfte, bzw. deren analoge Verwendung, sind nur bis zum Ende des jeweils nächsten Schuljahres zulässig, sofern keine Rechtsbehelfe oder Rechtsmittel zum Beispiel gegen ein Abschlusszeugnis eingelegt worden sind.
  Danach müssen alle personenbezogenen Daten gelöscht werden (außer Sie haben eine Einwilligung der Eltern/Schüler für eine längere Nutzungsdauer z.B. für Fotos/Videos).
- Werden personenbezogene Daten in Akten, Notenbücher, usw. verarbeitet, dann müssen Maßnahmen getroffen werden, um sicherzustellen, dass Unbefugte auf diese Daten bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung nicht zugreifen können (z.B. verschlossene Schublade, abgeschlossenes Zimmer, verschlossene Tasche).
  Probeausdrucke oder Fehldrucke sollten daher entweder zu Hause oder in der Schule (evtl. durch einen Dienstleister) angemessen entsorgt werden (schreddern).
- Der häusliche PC muss bei Nutzung durch Dritte (z.B. Ehegatte/Lebensparter) in verschiedene Benutzeroberflächen aufgeteilt werden! Die Anmeldung im schulrelevanten Teil muss passwortgeschützt sein.
- Datenschutzrelevante Daten sollten auf einem verschlüsselten USB-Stick bzw. auf einer verschlüsselten externen Festplatte abgespeichert werden. (Übergegen Sie sich hier: Was passiert, wenn der Rechner defekt ist? Wer repariert und erhält ggf. Zugriff auf sensible Daten?)
- Die Verfahren (Programme), die für die Schule freigegeben sind, dürfen auch zu Hause verwendet werden. Für die Verwendung aller anderen Verfahren (z.B. spezielle Programme) sind letztlich Sie als Lehrkraft selbst verantwortlich.
- Auf den IT-Systemen müssen ein Virenscanner mit ständiger Aktualisierung und eine Firewall installiert sein. Zudem müssen die Systeme auf dem aktuellen Stand gehalten werden (Einspielen von Updates, Patches, etc.).
- PCs oder Festplatten sollten nur verkauft oder an andere weitergegeben werden, wenn vorher alle Daten gelöscht wurden, mindestens durch ein mehrfaches Neuformatieren der Festplatte. **Dies ist aber immer noch kritisch- lieber die „Hammermethode“ anwenden.**

- Kollegen sollten davon absehen, Cloud-Systeme für personenbezogene Daten zu nutzen bzw. müssen diese Systeme die Anforderungen des Bayerischen Datenschutzes und der DS-GVO erfüllen.
- Auch Smartphones und ihre Verwendung für dienstliche Zwecke (z.B. Fotos, Videos, Kalender mit datenschutzrelevanten Daten) sind in der Hinsicht nicht unproblematisch. Bedenken Sie hier, dass Smartphones ihre Daten immer in der Cloud (sprich in den USA) sichern, außer Sie ändern die Einstellungen für die Cloudverwendung.
- Bei der Nutzung von Webportalen darf das eingegeben Passwort nicht im Browser für weitere Sitzungen gespeichert werden. Dies verhindert die unberechtigte Nutzung des Webportals durch andere Nutzen ihres privaten Umfelds, z.B. durch im Haushalt wohnende Kinder
- Bei der Nutzung offener Internetzugänge (z.B. in Internet-Cafés oder Hot-Spots an öffentlichen Plätzen) ist darauf zu achten, dass diese meist unverschlüsselt ihre Daten übermitteln. Nutzen Sie diese eher nicht für Ihre dienstliche Kommunikation bzw. sorgen sie für eine Verschlüsselung Ihrer Daten auf geeigneter Weise.
- Personenbezogene Daten sind nicht per E-Mail zu übermitteln, es sei denn, sie sind anonymisiert, pseudonymisiert oder verschlüsselt. Dies betrifft auch Zeugnisbemerkungen.

  Tipp 1: Worddokumente über „Datei"- „Dokument schützen"-„Mit Kennwort verschlüsseln" Das Kennwort sollte vorher vereinbart sein- das Schicken des Kennwortes in einer zweiten Mail ist nicht zu empfehlen.

  Tipp 2: Eine Zip-Datei erstellen, mit Passwort versehen und als Anhang verschicken;

  Tipp 3: Nicht alle E-Mail-Accounts sind geeignet für schulische Korrespondenzen. Der Server muss in Europa stehen. Konten von Google, Microsoft, etc. sind somit nicht verwendbar.

  Tipp 4: Fragen Sie bei Ihrer Schule nach, ob Sie eine Dienst-E-Mail erhalten können.

- Personenbezogene Daten sollten nur auf verschlüsselten Sticks transportiert werden.

Datenschutzvergehen müssen laut der DS-GVO beim Landesdatenschutzbeauftragen über die Schulleitung angezeigt werden. Versuchen Sie Verstöße zu vermeiden!