



Informationen zum digitalen Lernen und der digitalen Kommunikation zur Unterstützung hessischer Schulen im Zeichen der Covid-19-Pandemie

Die Schließung von Schulen, Hochschulen und anderen Bildungseinrichtungen führt zu verstärkter digitaler Kommunikation wie der Nutzung von E-Mail-Systemen, Messenger-Diensten oder der Anwendung von Videokonferenz-Applikationen und digitalen Lernplattformen – auch jeweils mit Cloud-Anbindungen. In allen Bereichen ist ein schnelles und zugleich umsichtiges Handeln erforderlich. Alle Maßnahmen sind mit Bedacht zu wählen. Der Datenschutz steht dem nicht entgegen.

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit will eine zeitlich befristete Nutzung von Privatgeräten durch die Anwender im häuslichen Bereich unter gewissen Rahmenbedingungen ermöglichen.

Die folgenden Anforderungen hinsichtlich der Nutzung der genannten Systeme und Dienste richten sich an Lehrkräfte, Erziehungsberechtigte sowie Schülerinnen und Schüler. Folgende Rahmenbedingungen sollten umgesetzt sein:

- Jede Kommunikation unter Verwendung personenbezogener Daten zur Unterstützung des pädagogischen Bereichs sollte möglichst datensparsam und zweckgebunden erfolgen.
- Es sollte möglichst keine Speicherung von sensiblen Daten auf dem Privatgerät erfolgen; im anderen Fall muss die Möglichkeit zur unkomplizierten und vollständigen Löschung der Daten bestehen.

Mobile Geräte müssen mindestens durch eine PIN oder ein Passwort geschützt sein (vgl. BSI für den Bürger unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html; letzter Aufruf: 23.03.2020)

- Sobald die Nutzung dieser Dienste nicht mehr erforderlich ist, sind die damit verarbeiteten personenbezogenen Daten zu löschen, insbesondere die zu diesem Zweck gespeicherten Telefonnummern von privaten Geräten. Dazu gehören speziell auch hierfür eingerichtete Kennungen web-basierter Applikationen, E-Mail-Adressen zur zwischenzeitlichen Nutzung oder deren Alias sowie (Arbeits-)Verläufe im Browser und dessen Cache.
- Bei Diensten und Systemen, die über eine Cloud-Anbindung verfügen, sind grundsätzlich diejenigen zu bevorzugen, die bei einer öffentlichen Stelle (wie z.B. das Hessische Schulportal) gehostet werden. Dies gilt insbesondere für Cloud-Speicher.
- Stehen solche im öffentlichen Bereich gehosteten Cloud-Lösungen nicht zur Verfügung, dann sind jedenfalls Systeme und Dienste einzusetzen,
 - o die eine Transportverschlüsselung sicherstellen und
 - o die Werkzeuge zur Inhaltsverschlüsselung anbieten. Sind keine Werkzeuge vorhanden, sollten die Anwenderinnen und Anwender selbst eine Inhaltsverschlüsselung der Dokumente mit Hilfe einer Applikation auf ihrem Privatgerät durchführen.
- Es ist darauf zu achten, dass Vertraulichkeit und Verfügbarkeit der Systeme und Dienste auf Dauer und unter Belastung sichergestellt ist. Ebenso sollte die Integrität personenbezogener Daten gewährleistet sein.
- Der schulinterne Datenschutzbeauftragte sollte beteiligt werden.