Datenschutzrechtliche Hinweise
zur Nutzung eines elektronischen Tage- oder Klassenbuchs (ETB)

1. Allgemeines

Das Klassen-, Lerngruppen- oder Kurstagebuch kann auch elektronisch geführt werden. Hierfür ist eine datenschutzkonforme Softwareanwendung zu wählen. Diese Handreichung unterstützt Sie bei der Auswahl und dem Betrieb einer solchen Softwareanwendung und macht Vorgaben zur grundsätzlichen Konfiguration.

Beim ETB ist sicherzustellen, dass die Datensätze der Klassen- und Kursbücher jederzeit an der Schule verfügbar sind. Es besteht die Verpflichtung, in regelmäßigen Abständen die gespeicherten Inhalte auszudrucken und in dieser Form zu archivieren.

Verschiedene Softwareanwendungen bieten ein elektronisches Klassenbuch (ETB) an. Meist als Modul zu einer komplexen Informations- und Kommunikationsplattform.

Diese Handreichung bezieht sich alleine auf den Betrieb eines ETB. Die weiteren Funktionsmöglichkeiten der Informations- und Kommunikationsplattformen werden nicht berücksichtigt.

2. Datenschutzrechtliche Problematik

In einem ETB werden personenbezogene Daten geführt, welche hohe Anforderungen an den Datenschutz stellen. Der unbefugte Zugriff auf diese Daten muss verhindert werden. Hierfür ist einerseits der Anbieter, andererseits aber auch die Schule verantwortlich.

Beim Betrieb des ETB muss darauf geachtet werden, dass nur die erforderlichen Daten verarbeitet werden. Dies sind:

a. Allgemein
   - Unterrichtsfach (Abkürzung)
   - Name der Lehrkraft (Kurzzeichen)
   - Unterrichtsgegenstand
   - Hausaufgaben
   - etwaige Bemerkungen

b. Schülerinnen und Schüler
   - Vor- und Nachname
   - Geburtsdatum

- Klassenzugehörigkeit
- Gruppenzugehörigkeit (Fachunterricht)
- Unterrichtsversäumnisse der Schüler
- Einträge zum Verhalten im Unterricht

c. Lehrkräfte
   - Vor- und Nachname
   - Fehlzeiten (mit Grund für Abwesenheit)
   - Stundenkontingent
   - unterrichtende Klassen
   - unterrichtete Fächer

Weitere personenbezogene Daten sind nicht im ETB zu hinterlegen. Hierfür werden die Schulverwaltungsprogramme genutzt.

ⓘ Einzelne ETB-Module bieten Einsichtsrechte für Eltern an. Hierfür ist teilweise das Hinterlegen einer E-Mail-Adresse der Eltern notwendig. Diese Datenerhebung ist nur mit Einwilligung der Eltern möglich. Bitte beachten Sie zu dieser Thematik die Hinweise unter Punkt 6b.

3. Netzinfrastruktur

Die erforderliche Netzinfrastruktur hängt davon ab, wo die Daten gespeichert werden. Bei der Gestaltung der schulischen Netzwerke sind die Vorgaben des Netzbriefs in seiner aktuellen Fassung zu beachten.

ⓘ Im Regelfall werden die Daten des ETB auf einem Server des Dienstleisters gespeichert. Hierbei handelt es sich um eine **Datenverarbeitung im Auftrag** nach Art. 28 DSGVO. Die Schule muss deshalb einen Vertrag zur Auftragsdatenverarbeitung abschließen. Ein Muster hierzu wird vom Kultusministerium zur Verfügung gestellt. (https://it.kultus-bw.de)

Werden die Daten **an der Schule** selbst gespeichert, muss das elektronische Tagebuch in einem eigenen physikalischen oder virtuellen Netz verortet werden. Die Verortung im „Lehrernetz“ ist nicht möglich, da ein Zugriff auf diese Umgebung vom Klassenzimmer aus unzulässig ist. Der Zugriff auf dieses eigene Netz ist so zu beschränken, dass nur auf die Bedienoberfläche des ETBs zugegriffen werden kann.
Der Zugriff kann auch über ein eigenes, gut abgesichertes WLAN erfolgen (WPA2-Enterprise nach 802.11i mit persönlicher Authentifizierung über ein X.509-Zertifikat nach 802.1X, mind. 15 Zeichen lange, komplexe Passphrasen – WLANs mit WPA2-Personal sind nicht ausreichend).
Die Einrichtung eines unidirektionalen Zugriffs vom Verwaltungsnetz aus ist zulässig.

4. Verschlüsselung

Die Datenübermittlung von den Endgeräten der Lehrkräfte in das ETB muss nach dem Stand der Technik verschlüsselt erfolgen.

5. Authentifizierung

Für die Authentifizierung ist neben Benutzername und Kennwort eine weitere Authentifizierung nötig - die 2-Faktor-Authentifizierung. Dies kann z. B. über einen Software-Token, Hardware-Token, One-Time-Password (OTP), Time-based One-time Password (TOTP) usw. bewerkstelligt werden.

- Bei Verwendung einer 2-Faktor-Authentifizierung auf Basis von Einmalpasswörtern (OTP- bzw. TOTP-Verfahren) ist zu deren Erzeugung grundsätzlich ein **zweites Gerät zwingend** erforderlich. Dieses Gerät muss sich im persönlichen Besitz der Lehrkraft befinden. Die Lehrkraft hat für einen Zugriffsschutz entsprechend dem Stand der Technik zu sorgen. Sofern sich das Gerät, mittels dem auf das ETB zugegriffen werden soll, im ausschließlichen persönlichen Besitz der Lehrkraft befindet (also z. B. ein Tablet, das alleine von dieser Lehrkraft genutzt wird und nicht im Klassenzimmer verbleibt), ist es zulässig, dass der zweite Faktor auch auf diesem Gerät erzeugt wird.
  Zudem sollen nur Softwareanwendungen zur Erzeugung dieser Einmalpasswörter genutzt werden, welche aus der EU bzw. EWR-Raum stammen (Geltungsbereich der EU-DSGVO). Es wird empfohlen, keine Softwarelösungen von Anbietern aus Drittstaaten (z.B. USA, China, Russland,) zu verwenden.
- Bleibt das Endgerät, das für die Eingabe bestimmt ist, stationär im Klassenzimmer, scheidet die Möglichkeit der Authentifizierung über ein auf dem Computer abgelegtes **Clientzertifikat** aus, weil dann das Risiko eines unbemerkten Diebstahls zu groß ist.
  Zur Nutzung von Clientzertifikaten wird eine "Certificate Authority (CA)" benötigt, die ein solches Zertifikat vergibt und zur jeweiligen Authentifizierung verifiziert. Dabei ist darauf zu achten, dass für den Fall dass zur CA personenbezogene Daten übermittelt werden, dies eine Datenverarbeitung im Auftrag darstellt. Es darf also kein Anbieter außerhalb der EU beauftragt werden.
  Für den Vertrag nach Art. 28 DSGVO kann die Vorlage des Kultusministeriums genutzt werden.
- Der Nutzer ist verpflichtet, das **Token** sorgsam zu verwahren und gegen Diebstahl zu schützen. Beim Hardware-Token muss sichergestellt sein, dass dieser nicht vervielfältigt werden kann.
- Der Verlust des "Schlüssels" ist vom Nutzer unverzüglich anzuzeigen, damit er für die Authentifizierung gesperrt werden kann. Er wird damit also für einen potentiellen Dieb wertlos.
- Regelmäßig, abhängig vom Einsatzszenario, muss eine Bestätigung der Anmeldung als Folge eines auto-Logouts erfolgen.
- Bei Verwendung einer 2-Faktor-Authentifizierung auf Basis von E-Mails dürfen diese E-Mails nicht per Mail-Client auf dem Gerät abgerufen werden, auf dem das E-Tagebuch genutzt wird. Bei Abruf der E-Mails

per Webbrowser auf dem gleichen Endgerät, dürfen die Zugangsdaten nicht im Browser gespeichert werden. Die Nutzerkennung und das Passwort des E-Mail-Accounts müssen sich von den Zugangsdaten des E-Tagebuchs unterscheiden.
- Eine neue Authentifizierung mittels zweiten Faktor muss mindestens einmal pro Tag erfolgen. Bei Anmeldung auf einem anderen Endgerät muss der zweite Faktor jedes Mal abgefragt werden.
- Bei einer Kombination von Elektronischem Tagebuch mit weiteren Funktionen in einer einzigen Softwarelösung, etwa einem Messenger oder Elterninformations-App muss der Zugang zum ETB separat über einen zweiten Faktor erfolgen.

Das Benutzerpasswort muss aus mindestens zehn Zeichen bestehen. Neben Groß- und Kleinbuchstaben sollte das Passwort auch Ziffern und Sonderzeichen enthalten. Bei der Erstanmeldung am ETB muss das Initialpasswort geändert werden.

6. Steuerung der Zugriffe/ Berechtigungen

a. Zugriff von Mitarbeiterinnen und Mitarbeitern der Schule (intern)
Im ETB sind vielfältige personenbezogene Daten abgelegt. Der Zugriff muss so geregelt sein, dass lediglich auf jene Daten zugegriffen werden kann, welche zur dienstlichen Aufgabenerfüllung erforderlich sind. Das ETB muss deshalb über ein Rechte- und Rollenkonzept zur Zugriffssteuerung verfügen. Hierbei muss mindestens zwischen folgenden Rollen unterschieden werden:
    - Administrator
    - Schulleitung
    - Mitarbeiterinnen und Mitarbeiter der Schulverwaltung
    - Klassenlehrkräfte
    - Fachlehrerinnen und Fachlehrer

   Die Zugriffsrechte für die entsprechenden Rollen entnehmen Sie bitte der unten angefügten Tabelle.

b. Zugriff von Eltern, Schülerinnen und Schülern (extern)
Erziehungsberechtige, Schülerinnen und Schüler können ein Interesse daran haben, auf bestimmte Informationen zuzugreifen. Die Schule entscheidet hierbei, ob sie aus pädagogischen Gründen einen solchen Zugriff gestattet. Dabei sind folgende Rechte aus Schülersicht möglich:
    - Einsichtsrecht in die eigenen Stammdaten
    - Einsichtsrecht in die eigenen Hausaufgaben
    - Einsichtsrecht in die eigenen Fehlzeiten

   Ein Zugriff auf die Eintragungen zum Unterrichtsfach, zur unterrichtenden Lehrkraft und zum Unterrichtsgegenstand darf nicht erfolgen.

   Die Authentifizierung des Elternzugriffs erfolgt ebenfalls durch ein Passwort (Anforderungen an Benutzerpasswörter s. Punkt 5).

7. Protokollierung

a. **Eingabeprotokollierung:** Es muss protokolliert werden, welche Daten zu welcher Zeit von wem in das elektronische Tagebuch eingegeben worden sind (dies umfasst die Eingabe, Veränderung und Löschung der Daten).

b. **Zugriffs- und Übermittlungskontrolle:** Es muss protokolliert werden, welcher Nutzer sich wann an das System angemeldet hat und auf welche Daten zugegriffen wurde.

c. **Speicherkontrolle:** Es ist zu empfehlen, dass sämtliche Daten in verschlüsselter Form gespeichert werden.

8. Administration

Aufgrund der umfangreichen Funktionen der Anwendungen und des, wie oben beschrieben, komplexen Rollen- und Rechtekonzepts erfordert insbesondere die Ersteinstellung der Anwendung ein umfangreiches Wissen über die Konfiguration und Bedienung des jeweiligen Programms.
Zudem hat der Administrator weitreichende Berechtigungen um Einsicht in Anmelde- und Protokolldaten zu nehmen.
Deshalb sollten bei der Auswahl des Administrators folgende Punkte berücksichtigt werden:

- Administrator ist nicht Mitglied der Schulleitung
- Der Administrator verfügt über gute Fachkenntnisse in der eingesetzten Software
- Regelmäßige Fortbildungen müssen ermöglicht werden
- Der Administrator gibt eine gesonderte Verschwiegenheitserklärung zur Leistungs- und Verhaltenskontrolle ab
- Die Administratorenrolle wird nur auf die notwendigsten Personen begrenzt

ⓘ Steht an der Schule keine Lehrkraft zur Verfügung, welche die obengenannten Voraussetzungen erfüllt, sollte die Einführung eines ETB kritisch geprüft werden.

Muster für ein Rechte- und Rollenkonzept

Daten	SL	SV	KL	FL	Admin	SuS/E
Stammdaten SuS	B	B	E[2]	E[2]	B	E[1]
Stammdaten LuL	B	E	E[1]	E[1]	B	-
Organisationsplanung (Raumbelegung, Prüfungsplanung…)	B	B	B	B	B	-
Anwesenheit/Fehlzeiten SuS (mit Bemerkungsfeld)	B	B	B	B	B	E[1]
Anwesenheit/Fehlzeiten LuL (mit Bemerkungsfeld)	B	B	E[2]	E[1]	B	-
Einträge zum Verhalten SuS im Unterricht	E	-	E[2]	B[2]	B	-
Einträge zum Unterrichtsgegenstand	E	-	E[2]	B[2]	B	-
Einträge zur unterrichteten Stunde	E	-	E[2]	B[2]	B	-
Hausaufgaben	E	-	E[2]	B[2]	B	E[1]
Systemeinstellungen und Protokolldateien	-	-	-	-	B	-

SL = Schulleitung
SV = Schulverwaltung
KL = Klassenlehrkraft
FL = Fachlehrkraft
Admin = Administrator
SuS/E = Schülerinnen und Schüler/Eltern

B = Bearbeitungsrechte
E = Einsichtsrechte
[1] = bezieht sich nur auf die Eintragungen zur eigenen Person
[2] = bezieht sich auf Eintragungen der unterrichteten Klassen
- = keine Berechtigung