Bayerisches Staatsministerium für
Unterricht und Kultus

Kommunikations- und Kollaborationswerkzeuge

Stand: 24.04.2024

→ www.km.bayern.de / gestalten / digitalisierung / datensicherheit / dienstliche-verwendung-digitaler-werkzeuge

Inhaltsverzeichnis

Dienstliche Verwendung digitaler Kommunikations- und Kollaborationswerkzeuge

Für die Erledigung dienstlicher Aufgaben kann auch in der Schule auf digitale Kommunikations- und Kollaborationswerkzeuge zurückgegriffen werden.

Da bei der Aufgabenerfüllung mitunter sensible personenbezogene Daten verarbeitet werden, muss auch ein besonderes Augenmerk auf die Datensicherheit gelegt werden.

Im Folgenden werden digitale Kommunikations- und Kollaborationswerkezeuge

- Groupware (z. B. E-Mail-Postfach, Kalender, Notizen),
- Messenger
- Cloud-Speicher
- Videokonferenzwerkzeuge

näher betrachtet und technische und organisatorische Maßnahmen beschrieben. Die Maßnahmen orientieren sich an den Anforderungen des BSI IT-Grundschutzes. Die Umsetzung der Maßnahmen stellen die Mindestsicherheitsstandards dar. Die Pflicht zur Umsetzung der in Nr. 6 Anlage 2 Abschnitt 7 zu § 46 BaySchO festgelegten technischen und organisatorischen Maßnahmen bleibt unberührt.

Die Zielgruppe der beschriebenen Maßnahmen ist: Schulleitung, pädagogischer Systembetreuer, Dienstleister, Lehrkräfte und sonstige an der Schule

tätiges Personal , Schulaufwandsträger

Regelung zur Datenverarbeitung und Rechenschaftspflicht der Schule

Die Schule legt innerhalb des Rahmens der gesetzlichen Vorgaben auf Basis ihrer Organisationshoheit fest, welche Daten mittels welchem digitalen Kommunikations - und Kollaborationswerkzeugs verarbeitet werden dürfen.

Dies dient dazu, dass die Schulleitung ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 i.V.m. Art. 32 DSGVO nachkommt.

Das Staatsministerium hat zu diesem Zweck die bereitgestellten (Muster-)Verarbeitungsbeschreibungen überarbeitet. Diese müssen an den dafür vorgesehenen Stellen ausgefüllt, zum Verarbeitungsverzeichnis genommen und bei Änderungen entsprechend aktualisiert werden.

Zielgruppe: Schulleitung

Kategorisierung des Schutzbedarfs

Gemäß IT-Grundschutz-Methodik des BSI hängen die für einen sicheren Einsatz von Kommunikations- und Kollaborationswerkzeugen notwendigen Maßnahmen vom Schutzbedarf der
darin verarbeiteten Daten ab.

Dabei unterscheidet man zwischen

- normalem Schutzbedarf (Regelfall)
- hohem Schutzbedarf, z.B. bei der Verarbeitung von Daten, die einem besonderen strafrechtlichen Geheimnisschutz
  unterliegen (z. B. § 203 StGB) (vgl. Nr. 3.4 Anlage 2 Abschnitt 7 zu § 46 BaySchO), bei der Verarbeitung von besonderen Kategorien personenbezogener Daten i. S. d. Art. 9 DSGVO, insbesondere Gesundheitsdaten (vgl. Nr. 3.4 Anlage 2 Abschnitt 7 zu § 46 BaySchO)

Folgende Tabelle stellt einen Überblick über in der Schule verarbeitete Daten (excl. der oben bereits genannten Daten) und deren Schutzbedarf dar.

Zielgruppe: Schulleitung, pädagogischer Systembetreuer, Dienstleister, Lehrkräfte und sonstiges an der Schule tätiges Personal

Überblick über in der Schule verarbeitete Daten mit ihrer Schutzbedarfskategorie

normal

- Allgemeine Bekanntmachungen
- Vorbereitung und Nachbereitung von Fortbildungen
- Vorbereitung und Nachbereitung von Fachsitzungen
- Bericht zur allgemeinen Klassensituation, ohne konkreten Bezug zu Einzelpersonen
- Unterrichtsmaterialien
- Informationen zu beurteilungs-relevanten Themen wie Nachweise zu besuchten Fortbildungen bzw. außerschulischen Aktivitäten (nicht die Beurteilung selbst!)
- Informationen im Zusammenhang mit dem Sachaufwand
- Einzelnoten
- Fehlzeiten ohne Bezug zum Gesundheitszustand

hoch

- Krankmeldungen
- Informationen über familiäre und soziale Hintergründe und soziale Beziehungen von Schülerinnen und Schülern oder Lehrkräften
- Informationen über Ordnungsmaßnahmen
- Kommunikation über das Verhalten einzelner Schülerinnen und Schüler
- Notenlisten

Der Umgang mit Einzelnoten und Notenlisten ist in den FAQ entsprechend geregelt.

HINWEIS

Aufgrund der heterogenen Schullandschaft kann die Vollständigkeit vom Staatsministerium für Unterricht und Kultus nicht gewährt werden. In Einzelfällen, die in der Tabelle nicht erfasst sind, muss die Schule selbstständig eine Schutzbedarfsfeststellung vornehmen, um die notwendigen Maßnahmen zu ergreifen.

Hierzu dienen auch die Hinweise zur Schutzbedarfsfeststellungen in den Downloads

Betrieb, Authentifizierung und Datenübertragung

Betrieb

Die digitaler Kommunikations- und Kollaborationswerkzeuge müssen sicher betrieben werden. Die relevanten Vorgaben ergeben sich aus dem IT-Grundschutz Kompendium (in der aktuellsten Fassung) und müssen vom Verantwortlichen umgesetzt werden.

Dazu zählen unter anderem:

- Patch- und Schwachstellenmanagement
- Schutz vor Schadprogrammen
- Protokollierung
- Datensicherungsmanagement
- Detektionsmanagement
- Incidentmanagement

Sofern ein Dienstleister oder der Schulaufwandsträger für den Betrieb zuständig ist, muss sich die Schule die Umsetzung von Sicherheitsmaßnahmen schriftlich bestätigen lassen. Dies kann beispielsweise in einer Vereinbarung über die Auftragsverarbeitung (AVV) – konkret in den zu regelnden technischen und organisatorischen Maßnahmen - mit dem Dienstleister oder dem Schulaufwandsträger erfolgen.

Authentifizierung

Um den Zugriff von Unberechtigten auf die Daten, die mittels der Kommunikations-Kollaborationswerkzeuge verarbeitet werden, zu schützen, ist eine Authentifizierung vorzusehen (i.d.R. Benutzername und sicheres Passwort). Dies muss durch den Betreiber des digitalen und Kommunikations- und Kollaborationswerkzeugs sichergestellt sein.

Datenübertragung

Alle Daten, die zwischen den Kommunikationspartnern ausgetauscht werden, sind während der Übermittlung über das Internet zu verschlüsseln (Transportverschlüsselung über TLS). Dies muss durch den Betreiber des digitalen Kommunikations- und Kollaborationswerkzeugs sichergestellt sein. Der Stand der Technik ist bei der Verschlüsselung stets zu beachten und umzusetzen.

Weiterführende Informationen können unter der Rubrik Verschlüsselung eingesehen werden.

Die weiteren spezifischen Mindestanforderungen werden bei den einzelnen Kommunikations- und Kollaborationswerkzeugen genannt.

Groupware

Unter Groupware versteht man in diesem Kontext eine Anwendung mit folgenden Funktionen:

- E-Mail-Postfach
- Kalender
- Kontaktverzeichnis
- Aufgaben/Notizen

Da in Groupware unter anderem besonders vertrauliche Daten verarbeitet werden, sollte der Zugang mit einer spezifischen Authentisierung (z. B. 2-Faktor-Authentisierung) geschützt werden. Dies muss durch den Betreiber sichergestellt sein.

Wenn E-Mails unverschlüsselt übertragen werden, können sich nicht berechtigte Dritte leicht Zugriff auf den Inhalt verschaffen. Daher muss darauf geachtet werden, dass Inhalte sicher übertragen werden. Das gilt insbesondere dann, wenn die E-Mail personenbezogene Daten enthält.

Daher müssen folgende Maßnahmen bei der E-Mail-Kommunikation beachtet werden:

Diejenigen personenbezogenen Daten, die über die notwendigen Angaben zu Absender und Empfänger hinausgehen, müssen Ende-zu-Ende-verschlüsselt übertragen werden. Die technischen Voraussetzungen müssen durch den Betreiber bereitgestellt werden. Ansonsten muss die Erzeugung und Verschlüsselung der Inhaltsdaten mit Drittprodukten erfolgen.

Diese Maßnahmen sind einem OnePager zusammengefasst.

Hinweis

Die E-Mail-Kommunikation, die über das im Bayerischen Schulportal integrierte Outlook Web Access (OWA) erfolgt, ist von oben genannten Maßnahmen nicht betroffen, da andere Sicherheitsmaßnahmen umgesetzt wurden.

Die automatische Weiterleitung an ein privates Postfach ist verboten und sollte technisch durch den Betreiber des Groupware-Dienstes sichergestellt werden. Sofern dies nicht möglich ist, muss durch die Schulleitung eine organisatorische Regelung getroffen werden.

Die E-Mail-Kommunikation wird auch von Kriminellen in Form von Phishing-E-Mails ausgenutzt, um an sensible Informationen (Zugangsdaten, etc.) zu gelangen (Social Engineering). Zudem werden Dateien mit Schadsoftware als Anhang von E-Mails versendet. Falls solche E-Mails nicht durch Sicherheitsmechanismen gefiltert werden und die Dateien ausgeführt werden, wird die Schadsoftware „aktiviert“. Diese kann z.B. durch „Verschlüsselungstrojaner“ zu erheblichen Schäden für den schulischen IT-Systeme führen.

E-Mails mit schädlichem Inhalt können täuschend echt aussehen. Es gibt jedoch Anzeichen, an denen die betrügerischen E-Mails erkannt werden können.

Zielgruppe: Schulleitung, pädagogischer Systembetreuer, Dienstleister, Lehrkräfte und sonstige an der Schule tätige Personal

Ein Leitfaden zum Erkennen von Phishing-E-Mails befindet sich bei den Downloads

Aufgaben und Notizen sollen so wenig wie möglich personenbezogene Inhalte enthalten. Dokumente als Anhang einer Aufgabe, die Daten mit hohem Schutzbedarf enthalten, müssen gegen einen Fremdzugriff geschützt werden (vgl. OnePager).

Es wird empfohlen, Verweise auf Dokumente (z.B. Link auf ein Dokument im Cloud-Speicher) zu hinterlegen, deren Zugriff entsprechend geschützt ist.

Kalendereinträge (insbesondere Betreff und Textfeld) sollen so wenig wie möglich personenbezogene Inhalte enthalten. Dokumente als Anhang des Kalendereintrags, die Daten mit hohem Schutzbedarf enthalten, müssen gegen einen Fremdzugriff geschützt werden (vgl. OnePager).

Kalenderfreigaben sind restriktiv zu setzen. Die Darstellung ist soweit nicht erforderlich auf die Anzeige „frei“ oder „gebucht“ einzuschränken.

Messenger

Beim Messenger werden organisatorische und technische Mindestanforderungen unterschieden. Die technischen Anforderungen müssen durch den Betreiber des Werkzeugs sichergestellt sein.

Der Name von Chatgruppen soll keine identifizierenden Informationen zu Personen oder dem besonders vertraulichen Inhalt enthalten.

Der Zugriff auf die lokal gespeicherten Nachrichten im Messenger (z.B. auf einem Smartphone) muss durch angemessene Maßnahmen geschützt werden (z. B. Pin-Eingabe beim Öffnen der Anwendung).

Daten dürfen nur über Messenger ausgetauscht werden, wenn sichergestellt ist, dass nur die Berechtigten (i. d. R. Absender und Empfänger) Zugriff auf diese Daten haben. Es ist eine Ende-zu-Ende-Verschlüsselung vorzusehen. Der Stand der Technik ist bei der Ende-zu-Ende-Verschlüsselung stets zu beachten und umzusetzen. Eine Ausnahme ist für die Überprüfung auf Schadsoftware gestattet . Der Zugriff auf die Metadaten, die beim Austausch von Nachrichten anfallen, ist nur den Berechtigten gestattet.

Bei Verlust des Endgeräts sollte es möglich sein, die Chatverläufe durch die Administration zu löschen.

Cloud-Speicher

Unter einem Cloud-Speicher versteht man in diesem Kontext einen Speicherort und/oder eine Austauschplattform einschließlich integrierter Kollaborationswerkzeuge, wie z.B. Weboffice.

Wird ein Cloud-Speicher als Speicherort genutzt, ist dieser für den schulischen Einsatz in einen

- Verwaltungsbereich und
- einen pädagogischen Bereich

zu unterteilen.

Der Zugang zum Cloud-Speicher und der Zugriff auf Daten, auch auf solche im „Papierkorb“ und in Backups, ist generell in einem Rollen- und Berechtigungskonzept restriktiv zu regeln.

Die Unterteilung des Cloud-Speichers in einen Verwaltungsbereich und einen pädagogischen Bereich muss nicht durch zwei physisch getrennte Systeme erfolgen, sondern kann auch über ein restriktives Rollen- und Berechtigungskonzept umgesetzt werden.

Sofern die Realisierung des Verwaltungsbereichs über ein restriktives Rollen- und Berechtigungskonzept erfolgt, müssen die Verzeichnisse, die dem Verwaltungsbereich zugeordnet sein sollen, eindeutig und unterscheidbar bezeichnet werden.

Da der Verwaltungsbereich besonders vertrauliche Daten enthalten kann, ist der Zugang zum Verwaltungsbereich mit einer spezifischen Authentisierung (z. B. 2-Faktor-Authentisierung) zu schützen. Die Daten im Ruhezustand müssen im Verwaltungsbereich des Cloud-Speichers durch eine Verschlüsselung geschützt werden. Der Stand der Technik ist bei der Verschlüsselung stets zu beachten und umzusetzen. Dies muss durch den Betreiber des Cloudspeichers sichergestellt sein. Liegen beide Bedingungen vor, dürfen Daten mit hohem Schutzbedarf ohne weitere Maßnahmen im Verwaltungsbereich abgelegt werden.

Im pädagogischen Bereich ist eine Verschlüsselung nicht zwingend erforderlich. Diese wird aber empfohlen. Der Zugang zum pädagogischen Bereich kann rollenspezifisch mit einer spezifischen Authentisierung (z. B. 2-Faktor-Authentisierung für Lehrkräfte) geschützt werden.

Der Zugang zum Cloud-Speicher sollte rollenspezifisch mit einer spezifischen Authentisierung (z. B. 2-Faktor-Authentisierung für Lehrkräfte) versehen werden.

Die Daten im Ruhezustand müssen im Cloud-Speichers durch eine Verschlüsselung geschützt werden. Der Stand der Technik ist bei der Verschlüsselung stets zu beachten und umzusetzen. Dies muss durch den Betreiber des Cloudspeichers sichergestellt sein.

Sofern die Daten im Ruhezustand des Cloud-Speichers nicht durch Verschlüsselung und mit einer spezifischen Authentisierung geschützt sind, dürfen Dokumente, die Daten mit hohem Schutzbedarf enthalten, nur verschlüsselt abgelegt werden. Die Verschlüsselung ist mit einem Drittprodukt durch den Endanwender umzusetzen.

Die vorangestellten Maßnahmen für den Cloudspeicher sind auch für ausschließliche Nutzung als Austauschplattform anzuwenden.

Berechtigten Dritten darf der Zugriff auf die Daten nur zeitlich begrenzt (z.B. begrenzte

Gültigkeitsdauer oder beschränkte Anzahl an Aufrufen) durch einen Link (für Externe) oder eine Berechtigung erteilt werden. Der Zugriff über einen Link soll passwortgeschützt erfolgen. Werden Daten mit hohem Schutzbedarf ausgetauscht, muss der Link passwortgeschützt sein. Die Übertragung des Passworts und des Links müssen über unterschiedliche Kommunikationswege erfolgen.

Die vorangestellten Maßnahmen für den Cloudspeicher sind auch für ausschließliche Nutzung als Austauschplattform anzuwenden.

Daten mit hohem Schutzbedarf dürfen kollaborativ verarbeitet werden, sofern sichergestellt ist, dass die Daten während der Bearbeitung durchgehend verschlüsselt sind. Eine geeignete Verschlüsselung mit entsprechendem Schutzniveau muss durch den Betreiber des Cloudspeichers sichergestellt sein.

Videokonferenzwerkzeug

Beim Videokonferenzwerkzeug werden organisatorische und technische Mindestanforderungen unterschieden. Die technischen Anforderungen müssen durch den Betreiber des Werkzeugs sichergestellt sein.

Der Name des einzurichtenden Videokonferenzraums soll keine identifizierenden Informationen zu Personen oder dem besonders vertraulichen Inhalt enthalten.

Unberechtigter Zugang zur Videokonferenz ist über einen personalisierten Einwahllink oder durch die Aktivierung des Warteraums zu verhindern. Dies gilt insbesondere auch bei Beratung und die Beschlussfassungen schulischer Gremien mittels Videokonferenzen (§ 18a BaySchO).

Die Teilnehmerinnen und Teilnehmer müssen sich angemessen und geeignet authentisieren. Dies kann zum Beispiel mittels Bild- und/oder Tonübertragung erfolgen.

Daten mit hohem Schutzbedarf dürfen nur über ein Videokonferenzwerkzeug ausgetauscht werden, wenn eine hinreichende Absicherung gegen Zugriffe über die Server des Anbieters vorgesehen ist. Diese Vorgabe gilt als erfüllt, wenn das Videokonferenzwerkzeug zentral vom Freistaat Bayern über das Staatsministerium bereitgestellt wird oder eine Ende-zu-Ende-Verschlüsselung vorsieht, bei der die Schlüssel nur den Berechtigten (Teilnehmern der Videokonferenz) zugänglich sind.

Daten mit hohem Schutzbedarf dürfen nur über den Chat und/oder den Dateiaustausch innerhalb des Videokonferenzwerkzeugs ausgetauscht werden, wenn eine hinreichende Absicherung gegen Zugriffe über die Server des Anbieters vorgesehen ist. Diese Vorgabe gilt als erfüllt, wenn das Videokonferenzwerkzeug zentral vom Freistaat Bayern über das Staatsministerium bereitgestellt wird oder eine Ende-zu-Ende-Verschlüsselung vorsieht, bei der die Schlüssel nur den Berechtigten (Teilnehmern der Videokonferenz) zugänglich sind.

Zudem müssen nach Beendigung der Videokonferenz der Chat und die ausgetauschten Daten unwiderruflich gelöscht werden.

Besonders zur Geheimhaltung verpflichtete Personen

Besonders zur Geheimhaltung verpflichtete Personen im Schulbereich (z. B. Schulpsychologinnen und Schulpsychologen, Personalräte) stehen nicht nur in der besonderen Verantwortung eines Berufsgeheimnisträgers, sondern haben regelmäßig Umgang mit Daten mit hohem Schutzbedarf. Deren Kommunikation in dieser Funktion unterfällt zusätzlich den nachfolgenden Voraussetzungen, sofern Daten mit hohem Schutzbedarf ausgetauscht werden. Dies gilt entsprechend für Beratungslehrkräfte (vgl. insbesondere Abschnitt III Nr. 4.1. der Bekanntmachung des Bayerischen Staatsministeriums für Unterricht und Kultus über die Schulberatung in Bayern vom 29. Oktober 2001 (KWMBl. I S. 454, StAnz. Nr. 47), die zuletzt durch Bekanntmachung vom 17. März 2023 (BayMBl. Nr. 148) geändert worden ist). Beim Austausch von Daten muss sichergestellt werden, dass diese nur an Personen übertragen werden, denen gegenüber eine Offenlegung der Daten gestattet ist. Die Identität des Kommunikationspartners ist in geeigneter Weise zu überprüfen.

Sofern bereits Daten über Sender und/oder Empfänger den Vorschriften zum besonderen strafrechtlichen Geheimnisschutz unterfallen, muss eine Einwilligung ausdrücklich auch diesen Aspekt umfassen.

Eine Kommunikation von Funktionsträgern im Rahmen der entsprechenden Funktion, die einer besonderen Geheimhaltungsverpflichtung unterfallen, hat über ein eigenes, dafür vorgesehenes E-Mail-Postfach zu erfolgen. Dieses Postfach muss nach außen erkennbar der jeweiligen Funktion des Postfachinhabers zugeordnet sein.

Sofern bereits Daten über Sender und/oder Empfänger den Vorschriften zum besonderen strafrechtlichen Geheimnisschutz unterfallen, muss eine Einwilligung ausdrücklich auch diesen Aspekt umfassen.

Weitere Teilnehmerinnen und Teilnehmer dürfen nur nach ausdrücklicher Zustimmung der bisherigen Beteiligten in den Chatraum aufgenommen werden.

Nach Abschluss der Kommunikation über eine bestimmte Angelegenheit, ist der Chatverlauf und gegebenenfalls der Chat unverzüglich zu löschen.

Die im Rahmen der Funktion angelegten Ordner sind speziell zu bezeichnen.

Für jede Sitzung ist ein neuer Videokonferenzraum zu erstellen (Verbot der Doppelnutzung).

Personenbezogene Daten sind nach Beendigung der Sitzung aus der Teilnehmerverwaltung des Videokonferenzwerkzeugs, in der Regel durch Auflösung des Konferenzraums, unverzüglich vom Initiator der Konferenz zu löschen.

Spezielle Regelungen für besondere Personengruppen bleiben unberührt.

FAQ zu diesem Thema

E-Mail: Beim E-Mail-Versand sind keine weiteren Maßnahmen zu beachten, wenn nicht personenbezogene Daten im Textfeld oder als Anhang übertragen werden (z.B. Einzelnoten). In diesem Fall ist die Vorgehensweise unter FAQ 2a, 2b zu beachten.

Messenger: Die Übertragung über den Messenger ist möglich.

Kommunikationstool innerhalb einer Schulanwendung: Eine Übertragung ist ohne weitere Maßnahmen möglich, sofern der Zugriff auf die Anwendung passwortgeschützt und verschlüsselt (Transportverschlüsselung) erfolgt. (Siehe hierzu auch: Verschlüsselung)

E-Mail: Bei Einzelnoten ist ein E-Mail-Versand über das dienstliche E-Mail-Postfach ohne weitere Maßnahmen möglich, wenn der Absender und der Empfänger dieselbe E-Mail-Domäne verwenden (z.B. ...@schulen.bayern.de). Notenlisten hingegen haben einen hohen Schutzbedarf und müssen verschlüsselt werden. Das Passwort zum Entschlüsseln wird über einen gesonderten Kommunikationsweg (z. B. Messenger, Telefon) übermittelt. Die Umsetzungshinweise können Sie dem folgendem OnePager entnehmen.

Messenger: Eine Übertragung per Messenger ist bei Einzelnoten sowie Notenlisten ohne weitere Maßnahmen möglich.

Kommunikationstool innerhalb einer Schulanwendung: Eine Übertragung ist bei Einzelnoten sowie Notenlisten ohne weitere

Maßnahmen möglich, sofern der Zugriff auf die Anwendung passwortgeschützt und verschlüsselt (Transportverschlüsselung) erfolgt. (Siehe hierzu auch: Verschlüsselung)

E-Mail: Bei Noten ist beim E-Mail-Versand eine Verschlüsselung notwendig. Die Umsetzungshinweise können Sie dem folgenden OnePager entnehmen.

Messenger: Eine Übertragung per Messenger ist bei Einzelnoten sowie Notenlisten ohne weitere Maßnahmen möglich.

Kommunikationstool innerhalb einer Schulanwendung: Eine Übertragung ist bei Einzelnoten sowie Notenlisten ohne weitere Maßnahmen möglich, sofern der Zugriff auf die Anwendung passwortgeschützt und verschlüsselt (Transportverschlüsselung) erfolgt. (Siehe hierzu auch: Verschlüsselung)

E-Mail: Krankmeldungen haben einen hohen Schutzbedarf. Die Krankmeldung muss deswegen als Anhang verschlüsselt werden und kann anschließend versendet werden. Die Umsetzungshinweise können Sie dem folgenden OnePager entnehmen.

Messenger: Die Krankmeldung kann ohne weitere Maßnahmen an den Empfänger versendet werden.

Kommunikationstool innerhalb einer Schulanwendung: Eine Übertragung ist ohne weitere Maßnahmen möglich, sofern der Zugriff auf die Anwendung passwortgeschützt und verschlüsselt (Transportverschlüsselung) erfolgt. (Siehe hierzu auch: Verschlüsselung)

E-Mail: Entsprechende Informationen müssen verschlüsselt werden und können anschließend versendet werden. Die Erziehungsberechtigten sind diesbezüglich zu sensibilisieren.

Messenger: Die entsprechenden Informationen können ohne weitere Maßnahmen übertragen werden.

Verwaltungsbereich auf physisch getrennten Systemen: Es sind keine weiteren Maßnahmen erforderlich. Die Zugriffsberechtigungen müssen restriktiv eingestellt werden.

Einheitlicher Cloud-Speicher: Das Dokument muss in einem Verzeichnis, das dem Verwaltungsbereich zugeordnet ist, und verschlüsselt abgelegt werden. Die

Zugriffsberechtigungen müssen restriktiv eingestellt werden.

Hinweis: Der Verwaltungsbereich der BayernCloud Schule steht voraussichtlich im ersten Quartal 2025 zur Verfügung.

ja

Die Daten haben einen normalen Schutzbedarf und können auf jedem Kommunikations- und Kollaborationswerkzeug ohne weitere Maßnahmen übermittelt werden.

E-Mail-Austausch muss als unsicher eingestuft werden, da der Kommunikationspfad nicht vorhersagbar ist und Daten auch unverschlüsselt ausgetauscht werden könnten.
Eine Ausnahme bildet die Kommunikation über einen Webclient am gleichen Mailsystem (Bsp.: Zwei Lehrkräfte nutzen beide ByCS-Dienst-E-Mail).

Der Messenger bietet meist eine Ende-zu-Ende-Verschlüsselung. Die Nachrichten können in diesem Fall nur durch die beiden Kommunikationspartner im Klartext gelesen werden.

E-Mail: Für besondere Funktionen in der Schule gibt es Funktions-E-Mailadressen, Bsp.: Schulpsychologe, Beratungslehrkraft oder Personalrat.
Diese sind getrennt von persönlichen Postfächern zu führen. Diese speziellen Postfächer sind zu adressieren. Die Daten haben einen hohen Schutzbedarf und müssen verschlüsselt werden. Das Passwort zum Entschlüsseln wird über einen gesonderten Kommunikationsweg (z. B. Messenger, Telefon) übermittelt.

Messenger: Die Übertragung über den Messenger ist möglich.

Diese Vorgabe gilt als erfüllt, wenn das Videokonferenzwerkzeug zentral vom Freistaat Bayern über das Staatsministerium bereitgestellt wird oder eine Ende-zu-Ende-Verschlüsselung vorsieht, bei der die Schlüssel nur den Berechtigten (Teilnehmern der Videokonferenz) zugänglich sind

Downloads

Hinweise zur Schutzbedarfsfeststellung https://www.km.bayern.de/download/4-24-04/Schutzbedarfsermittlung.pdf

OnePager Sichere E-Mail-Kommunikation https://www.km.bayern.de/download/4-24-04/OnePager_sichere_E-Mail-Kommunikation.pdf

Leitfaden „Erkennen einer Phishing-E-Mail" https://www.km.bayern.de/download/4-24-04/Erkennen_von_Phishing_Mails.pdf