Baden-Württemberg
MINISTERIUM FÜR KULTUS, JUGEND UND SPORT
BADEN-WÜRTTEMBERG

Ministerium für Kultus, Jugend und Sport Baden-Württemberg
Postfach 10 34 42 ◆ 70029 Stuttgart

An alle
öffentlichen Schulen
des Landes Baden-Württemberg

Stuttgart April 2023
Durchwahl 0711 279-4222
Telefax 0711 279-2810
Name Thomas Eckert
Gebäude Thouretstrasse 6
Aktenzeichen 51-0551.0/35
(Bitte bei Antwort angeben)

nachrichtlich Abt. 7 der RPen, SSÄ,
LMZ, LS, Seminare und Akademien

Netzwerke an Schulen

Sehr geehrte Damen und Herren,

das Kultusministerium hat im Schreiben vom 16. Juni 2014, Az. 15-0551.0/34 (sogenannter Netzbrief 2) Informationen zur Gestaltung von Netzen an Schulen mitgeteilt. Der zunehmende Bedarf für die unterrichtliche Verwendung von sogenannten Kompetenzrastern machte es erforderlich, den Netzbrief in Bezug auf das Unterrichtsnetz fortzuschreiben. Die bisherigen Hinweise zur Gestaltung der Arbeitsumgebung Schulleitung (Verwaltungsnetz) und der Arbeitsumgebung Lehrkräfte (Lehrernetz) gelten unverändert weiter, während bei der Unterrichtsumgebung (Pädagogisches Netz) Ergänzungen notwendig sind. Eine weitere geringfügige Anpassung war aufgrund der EU-DSGVO erforderlich.

In Schulen werden die unterschiedlichsten personenbezogenen Daten verarbeitet. So erfolgt an Schulen neben der Speicherung personenbezogener Daten, die im Unterricht benötigt werden, auch die Verarbeitung von Daten der Schülerinnen und Schüler sowie der Sorgeberechtigten bis hin zu Bewertungen und Beurteilungen von Schülern im Rahmen der Schulverwaltung. Ferner werden auch personenbezogene

Daten der Lehrkräfte im Sinne der Personalverwaltung (z. B. dienstliche Beurteilungen) verarbeitet.
Wesentliches Ziel bei der Gestaltung der Netzinfrastruktur an Schulen ist es, diese unterschiedlichen personenbezogenen Daten besonders zu schützen. Dabei ist insbesondere sicherzustellen, dass nur diejenigen Personen auf solche personenbezogene Daten zugreifen können, die zur Erfüllung ihrer dienstlichen Aufgaben unbedingt erforderlich sind.

Das Kultusministerium empfiehlt aufgrund des technologischen Fortschritts und der Anforderungen von Schulen die Einrichtung einer **dreistufigen Netzinfrastruktur**, welche aus einer lokalen informationstechnischen Arbeitsumgebung für die Schulleitung, einer Umgebung für die Lehrkräfte und einer informationstechnischen Unterrichtsumgebung besteht. Zwischen diesen Netzen dürfen unter bestimmten Bedingungen Übergänge eingerichtet sein. Die Einrichtung von sog. VLANs (virtuellen Netzen) oder die Nutzung von Virtuellen Maschinen ist zulässig.

Nur in der "**Arbeitsumgebung Schulleitung"** (sogenanntes Verwaltungsnetz) dürfen ASV-BW oder andere Schulverwaltungsanwendungen, derzeit auch noch SVP-BW, betrieben werden. Nur in diesem Netz erfolgt die Verwaltung von Daten der Schüler und Schülerinnen, der Sorgeberechtigten und der Lehrkräfte sowie die Erledigung von hoheitlichen Aufgaben wie der Zeugniserstellung. Insbesondere ist es nur in dieser Arbeitsumgebung zulässig, dienstliche Beurteilungen von Lehrkräften zu verarbeiten.
Zugänge ins Internet müssen wie gehabt den Sicherheitsstandards von KVN oder LVN entsprechen. Sämtliche Computer dieser Arbeitsumgebung dürfen in dem an die KISS angeschlossenen Datennetz arbeiten. Es ist keine Trennung von KISS-PC und den anderen Verwaltungsrechnern erforderlich, insbesondere bei Schulleitung, Stellvertretung oder Sekretariat.

Die "**Arbeitsumgebung Lehrkräfte"** (sogenanntes Lehrernetz) soll den Lehrkräften zur Unterrichtsvorbereitung oder zum Sammeln und Gestalten von Unterrichtsmaterial dienen. Ferner erfolgt in diesem Netz die pädagogische Verwaltung: So können Lehrkräfte dort Bewertungen oder Benotungen von Schülerarbeiten verarbeiten und

speichern. Auch kann von hier aus der Zugriff z. B. auf das Verfahren "Kompetenzanalyse" erfolgen. Diese Daten müssen so gespeichert werden, dass nur dazu Befugte auf die zur Aufgabenerfüllung unbedingt erforderlichen Daten zugreifen können; dies könnte beispielsweise durch eine Zugriffberechtigungsstruktur in einem Dateisystem erfolgen.
Personenbezogene Daten von Lehrkräften, außer deren Name/Kürzel sowie die unterrichteten Klassen (z. B. Stundenpläne) dürfen in diesem Netz nicht verarbeitet werden. Computer der Arbeitsumgebung für Lehrkräfte dürfen sich nur in Räumen befinden, die ausschließlich für Lehrerinnen und Lehrer bestimmt (z. B. Lehrerzimmer) und abschließbar sind.
Vom Lehrernetz aus ist ein geregelter Zugriff in Richtung Schulverwaltungsnetz auf ausgewählte Ressourcen zulässig, wenn sichergestellt ist, dass keine personenbezogenen Daten vom Schulverwaltungsnetz dabei im Lehrernetz physikalisch abgelegt werden können.
Ein Zugriff durch Lehrkräfte vom Lehrernetz aus auf die Unterrichtsumgebung ist zulässig. Jeglicher Schülerzugriff auf das Lehrernetz ist unzulässig. Ein Zugriff vom Klassenzimmer aus auf dieses Netz ist zu verhindern.

In der **Unterrichtsumgebung** (sogenanntes pädagogisches Netz) können Schülerinnen und Schüler sowie Lehrkräfte aktiv sein. Es muss gewährleistet sein, dass ein Zugriff auf das Lehrernetz und Verwaltungsnetz vom pädagogischen Netz aus wirksam verhindert wird. Im pädagogischen Schulnetz dürfen ***grundsätzlich*** keine personenbezogenen Daten von Schülerinnen und Schülern verarbeitet und gespeichert werden, außer Name und Klassenzugehörigkeit der Schülerin/des Schülers sowie die hierzu erforderlichen technischen Daten, die direkt für die Unterrichtsgestaltung erforderlich sind. Insbesondere dürfen **grundsätzlich** keinerlei personenbezogene Daten zu Verhalten oder Leistung (Bewertungen, Beurteilungen) einer Schülerin/eines Schülers verarbeitet werden. Insgesamt dürfen in diesem Netz nur die zur Aufgabenerfüllung unbedingt erforderlichen Daten verarbeitet werden. Für die Unterrichtsumgebung empfiehlt das KM die Verwendung der paedML des Landesmedienzentrums BW.
Zeugnisse, Lernstandsberichte, Halbjahresinformationen und vergleichbare Dokumente dürfen in der Unterrichtsumgebung **generell** nicht verarbeitet werden.

Ist jedoch beabsichtigt, weitere personenbezogene Daten von Schülerinnen und Schülern in der Unterrichtsumgebung zu verarbeiten, beispielsweise laufende Leistungsbeurteilungen (Einteilung in Niveaustufen oder der Einsatz von Kompetenzrastern), müssen zwingend die folgenden technischen Datenschutzmaßnahmen getroffen werden.

- Eine Datenspeicherung in der Unterrichtsumgebung ist unzulässig. Die Datenspeicherung muss in einem eigenen Netz (auch VLAN) auf einem eigenen Server (auch virtueller Server) erfolgen. Ein auf die notwendigen Dienste begrenzter, dedizierter Zugriff vom pädagogischen Netz aus auf diesen Server ist auf Applikationsebene zulässig. Durch ein Berechtigungssystem ist sicherzustellen, dass jeder Benutzer nur Zugang zu den für ihn bestimmten Daten erhält. Die Datenspeicherung kann auch außerhalb des Schulnetzes, beispielsweise bei einem Dienstleister, erfolgen; in diesem Fall sind auch die Vorgaben für eine sog. Auftragsdatenverarbeitung nach Art. 28 EU-DSGVO zu beachten.
- Als Identitätsnachweis ist für jeden Nutzer eine Zwei-Faktoren-Authentifizierung erforderlich, die aus der Kombination von zwei verschiedenen voneinander unabhängigen Komponenten (Faktoren) besteht. Zusätzlich zum üblichen Passwort ist der Besitz eines "elektronischen Schlüssels" erforderlich. Denkbar wäre die Verwendung von Hardwaretokens oder von Einmal-Passwörtern (time-based one-time-Passwort, nach dem TOTP- bzw. OTP-Verfahren). Bei der Verwendung eines Einmalpassworts muss die Passworterzeugung grundsätzlich zwingend auf einem zweiten Gerät erfolgen. Dies gilt nicht für den Fall, dass das Gerät, mittels dem personenbezogenen Daten verarbeitet werden, ausschließlich einer Lehrkraft fest zugeordnet ist und von dieser Lehrkraft mitgeführt wird und nicht im Klassenzimmer verbleibt. In diesem Fall ist die Passworterzeugung auf demselben Gerät zulässig. Alternativ könnte auch eine TAN-Liste verwendet werden.
- Jede unverschlüsselte Übermittlung dieser personenbezogenen Daten im Unterrichtsnetz ist unzulässig. Die übertragenen Daten müssen vollständig Ende-zu-Ende verschlüsselt sein, d.h. sie werden auf dem gesamten Weg zwischen Server und Empfänger verschlüsselt.

Die einzelnen Netze bzw. Netzsegmente sind physikalisch oder logisch z. B. über Switches/Router oder Firewalls gegeneinander abzuschotten. Zugriffe über die Netze bzw. Netzsegmente hinweg sind in geeigneter Weise zu protokollieren.

Alternativ ist auch eine Netzinfrastruktur zulässig, die lediglich aus zwei Netzen besteht. Dabei ist jedoch zu beachten, dass nur die Umgebung für die Schulleitungsumgebung und Lehrkräfte zusammengefasst sein dürfen. Die Unterrichtsumgebung muss getrennt realisiert sein, ein Übergang in das andere Netz ist nicht zulässig.

Herstellerneutrale Beispiele und Hinweise für die Gestaltung der Netzwerkstruktur einer Schule finden Sie unter www.it.kultus-bw.de.

Mit freundlichen Grüßen

gez. Thomas J. Eckert
Regierungsdirektor