STADT FRANKFURT AM MAIN STADTSCHULAMT

Beschreibung pädagogisches WLAN an Frankfurter Schulen

Hinweise für Schulleitungen und IT-Beauftragte

Stadt Frankfurt am Main
- Der Magistrat -
Stadtschulamt
40.2 Informations- und Kommunikationstechnik
Solmsstraße 27-37
60486 Frankfurt am Main

E-Mail: it-servicedesk.amt40@stadt-frankfurt.de

Version 1.6

Dokumentinformation	
Dokumentenklasse:	Anleitung
Dokumententitel:	Beschreibung pädagogisches WLAN an Frankfurter Schulen
Dateiname:	Anleitung_WLAN
Version:	1.6
Letzte Bearbeitung:	24.03.2022 24.03.2022 16:48
Seitenzahl:	17

Inhaltsverzeichnis

1 Einleitung

Das Stadtschulamt Frankfurt am Main stellt den Schulen WLAN (Wireless Local Area Network, drahtloses lokales Netzwerk) für den pädagogischen Bereich zur Verfügung. Dieses Dokument stellt die wesentlichen technischen Informationen dazu zusammen, der letzte Abschnitt erläutert einige rechtliche Aspekte. Das Dokument wendet sich an die Schulleitungen und IT-Beauftragten, es ist nicht für den „Endnutzer“ gedacht.

An dieser Stelle wird das sog. „Universelle pädagogische WLAN“ beschrieben. Andere städtische WLAN-Netze, wie z. B. das freie „City-WLAN“ für Warte- und Museumsbereiche, sind nicht Gegenstand dieses Dokumentes und sind auch nicht für Schulen vorgesehen.

2 Überblick

2.1 Das Lernzonenmodell

Das von der Stadt Frankfurt am Main für die Schulen erstellte und durch die Stadtverordnetenversammlung genehmigte WLAN-Konzept sieht eine nach Schüler/innenzahl quotierte Anzahl von Access-Points (AP) vor. Die Quote beträgt 1:25 (AP zu Schüler/innen). Bei einer Klassengröße von 25 Schüler/innen entspricht dies rechnerisch einer Ausstattung aller Klassenräume einer Schule (ohne Fachräume und zusätzliche Unterrichtsräume). Hinzu kommt die Versorgung der Lehrerzimmer, nicht jedoch Lehrervorbereitungsräume. Bewusst stellt dies also keine flächendeckende Ausstattung mit WLAN („Vollausleuchtung“) dar, sondern WLAN steht nur in sog. Lernzonen zur Verfügung. Eine Lernzone umfasst z. B. einen Klassen- oder Fachraum, eine Aula, einen Aufenthaltsbereich oder eine abgegrenzte Zone in einer Sporthalle. So kann eine Schule festlegen, wo WLAN genutzt werden soll, und wo nicht. Jede Schule bestimmt die Lernzonen eigenständig anhand ihres pädagogischen Konzeptes. Die Positionierung der Access-Points geschieht dann nach technischen Gesichtspunkten innerhalb der Lernzone. Nur innerhalb der Lernzonen ist ein ausreichender WLAN-Empfang gewährleistet, außerhalb (z. B. im angrenzenden Flur) ist der Empfang zwar meist möglich, wird aber nicht garantiert und wird auch nicht vom Support abgedeckt. Grundsätzlich gilt: 1 Lernzone ist ein umbauter Raum, der in der Regel mit 1 Access-Point ausgestattet wird.

2.2 Drei Netze

In den Lernzonen werden drei WLAN-Netze zur Verfügung gestellt:

- Das pädagogische EDU-WLAN für die schuleigenen mobilen Endgeräte der Pädagogik (z. B. Notebooks, Convertibles, Tablets).
- Das BYOD-WLAN („Bring your own Device“) für die Nutzung von privaten Endgeräten der Lehrerschaft und/oder Schülerschaft.
- Ein Gast-WLAN für Gäste in der Schule. Dieser Zugang zum Internet ist über sogenannte Voucher zeitlich begrenzt. Die Voucher können über eine Administrationsoberfläche (Sponsorportal) von der Schule frei vergeben werden.

Die Access-Points in den Lernzonen senden stets alle drei Netze (SSID) aus. Ohne die für das jeweilige Netz vorgesehene Authentifizierung ist jedoch keines der drei Netze nutzbar, es handelt sich also nicht um „freie“ Netze. Dies schützt sie vor unautorisierter Nutzung von außen. Die Schulen haben über die Zulassung von Nutzern zum pädagogischen Netz und die Ausstellung von Vouchern die volle Kontrolle über die Nutzung der Netze.

Die weiteren Eigenschaften und Nutzung dieser Netze werden in den folgenden Abschnitten erläutert.

2.3 Bevor Sie WLAN bekommen

Die Ausstattung Ihrer Schule mit WLAN geschieht in der Regel im Rahmen einer generellen Erneuerung der Schul-IT. Dazu werden Sie vorher benachrichtigt und in einem Gespräch mit dem Rollout-Team des Stadtschulamtes über die Rahmenbedingungen und den Ablauf informiert. Dabei erfahren Sie auch die für Ihre Schule vorgesehene Anzahl von Lernzonen bzw. Access-Points. Die Lernzonen, d. h. die mit WLAN zu versorgenden Räume und Bereiche (s. 2.1), legen Sie selbst fest. Die genaue Positionierung der Access-Points wird während einer späteren Begehung des Schulgebäudes durch das durchführende Dienstleistungsunternehmen festgelegt. Dazu muss die Liste der gewünschten Lernzonen vorlie-

gen und die IT-Beauftragten sollen für Rückfragen zur Verfügung stehen. Bei der Auswahl der Lernzonen ist die maximale Anzahl zu berücksichtigen und der notwendige Anschluss an vorhandene Datendosen. In Bestandsgebäuden werden die Access-Points an eine Daten-Doppeldose angeschlossen, deren beide Anschlüsse zuvor zu einem zusammengelegt werden, damit die notwendige Datenrate und Versorgung mit Strom über das Netz gewährleistet sind. Es fällt also für WLAN eine Doppeldose im Raum weg. Für das pädagogische Netz ist dies meist kein Verlust, da WLAN als Netzzugang für mobile Geräte zur Verfügung steht. Dosen mit einem Telefonanschluss (VOIP) können nicht für WLAN genutzt werden. Aufgrund dieser Bedingungen und anderer baulicher Einschränkungen kann es vorkommen, dass während der Begehung die Lernzonenauswahl noch einmal geringfügig angepasst werden muss.

Bereiche des Schulgebäudes, die noch nicht netzwerktechnisch erschlossen sind, können erst WLAN bekommen, wenn die entsprechenden Verkabelungsarbeiten geplant, beauftragt und durchgeführt wurden. Dies gilt beispielsweise oft für Sporthallen. Möchten Sie in solchen Bereichen WLAN nutzen, kann dies zwar im Rahmen der Festlegung der Lernzonen gemeldet werden, die Umsetzung kann jedoch oft erst sehr viel später erfolgen. Für eine Übergangszeit haben Sie also weniger Lernzonen zur Verfügung als Ihrer Schule rechnerisch zustehen.

Die Einführung von WLAN an Ihrer Schule muss durch einen Beschluss der Schulkonferenz bestätigt werden. Sinnvollerweise entscheidet diese auch darüber, welche der drei WLAN-Netze an Ihrer Schule genutzt werden sollen. Informationen als Grundlage Ihrer Entscheidung finden Sie auch in den Abschnitten 6.3, 6.6, 6.7 und 8 dieser Dokumentation.

3 EDU-WLAN

3.1 Eigenschaften

Das EDU-WLAN ist ausschließlich für die schuleigenen, vom Stadtschulamt beschafften und betriebenen mobilen Endgeräte (z. B. Notebooks, Convertibles) bestimmt. Auf diesen Geräten ist das EDU-WLAN fest implementiert und sie verbinden sich in der Nähe eines Access-Points nach dem Einschalten und im Betrieb automatisch mit diesem Netz. Analog zu den stationären PCs melden sich Benutzer mit ihrem pädagogischen Benutzerkonto am Gerät an. Anschließend hat der angemeldete Benutzer den vollen Zugriff auf alle pädagogischen IT-Ressourcen wie z. B. Netzwerklaufwerke, Drucker, pädagogische Programme und das Internet, als wäre er/sie an einem PC im pädagogischen Netz angemeldet. Der Zugang zum Internet ist auf das HTTP/HTTPS-Protokoll beschränkt, Näheres dazu s. Abschnitt 6.4.

Bei Ausfall der Anbindung der Schule an das städtische Netz bleiben Verbindungen innerhalb des pädagogischen Netzes der Schule erhalten. Dadurch kann weiter per WLAN auf das pädagogische Netz (Anmeldung, Netzwerklaufwerke, Drucker) zugegriffen werden. Die Verbindung zum Internet ist in diesem Fall naturgemäß unterbrochen.

Die schuleigenen Geräte des pädagogischen Netzes können nur mit dem EDU-WLAN verbunden werden, andere WLAN-Netze (z. B. öffentliche oder private) sind auf den Geräten gesperrt.

3.2 Verbindungsaufbau

SSID (Netzname):	**EDU, EDU-GPO**
Netzwerkschlüssel:	**–**
Anmeldung:	*am Gerät wie im kabelgebundenen pädagogischen Netz (Windows-Anmeldung)*

Der Verbindungsaufbau erfolgt automatisch, die Nutzung des EDU-WLANs ist nach der Anmeldung im pädagogischen Netz möglich. Erfolgt die Anmeldung mit einem lokalen Benutzer (Standalone-Nutzerkonto), ist die Nutzung der Ressourcen des pädagogischen Netzes und des WLANs nicht möglich.

Die Authentifizierung der Geräte des pädagogischen Netzes erfolgt durch ein auf dem Gerät hinterlegtes digitales Zertifikat. Ist die Verbindung erfolgreich aufgebaut, wechselt die Anzeige der SSID von EDU auf EDU-GPO. Das Zertifikat besitzt eine zeitlich begrenzte Gültigkeit und muss deshalb regelmäßig über das Netzwerk erneuert werden. Dies ist – neben der Versorgung mit Updates – ein weiterer Grund dafür, dass die mobilen Geräte des pädagogischen Netzes regelmäßig mit dem stationären Netzwerk (z. B. im Notebookwagen) verbunden werden müssen. Bitte schließen Sie die mobilen Geräte einge-

schaltet an das Netzwerk an bzw. schalten Sie sie danach ein, damit die kabelgebundene Netzwerkschnittstelle aktiviert ist. Dazu finden Sie nähere Hinweise in der Anleitung und Nutzungsvereinbarung zu den Aufbewahrungssystemen, die Sie ebenfalls erhalten.

4 BYOD-WLAN

4.1 Eigenschaften

Das BYOD-WLAN wird zur Nutzung mit den privaten Geräten von Schulangehörigen (Lehrerschaft, Schülerschaft) zur Verfügung gestellt. Die erforderliche Anmeldung in diesem Netz erfolgt mit den vorhandenen Benutzerkennungen des pädagogischen Netzes. Ein Zugriff auf die IT-Ressourcen der Pädagogik (Netzwerklaufwerke, Drucker) ist aus Sicherheitsgründen nicht möglich.

Unter einem Account können maximal drei Geräte gleichzeitig mit dem BYOD-WLAN verbunden werden. Zurzeit bestehen keine Beschränkungen in den Nutzungszeiten oder des Datenvolumens. Werden im Verlauf der sukzessiven Hinzunahme weiterer Schulen in den WLAN-Betrieb Engpässe festgestellt, können sich hier ggf. Anpassungen ergeben. Eine Beschränkung des Zugangs (z. B. auf bestimmte Zeiten oder Räume, Benutzergruppen innerhalb des pädagogischen Netzes, Sperrung einzelner Zugänge) ist nicht möglich.

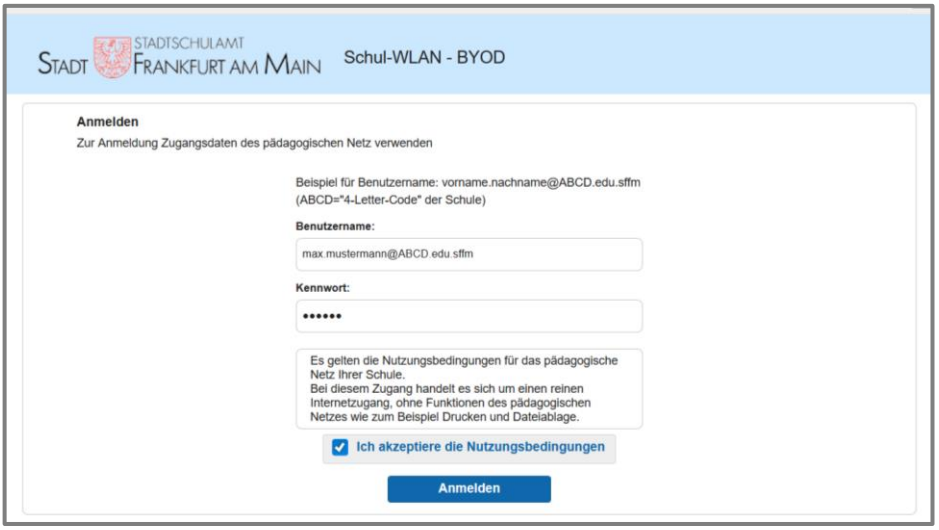
4.2 Verbindungsaufbau

SSID (Netzname):	**BYOD**
Netzwerkschlüssel:	*wird vom Servicedesk des Stadtschulamtes mitgeteilt*
Anmeldung:	*am Portal (Anmeldemaske) mit dem Konto des pädagogischen Netzes*

Der Netzwerkschlüssel wird jährlich zum Schuljahresbeginn geändert und den IT-Beauftragten vom Servicedesk des Stadtschulamtes mitgeteilt.

Die Verbindung mit dem Internet geschieht in zwei Stufen.

1. Verbindung mit dem WLAN, wie durch das Betriebssystem des Endgerätes vorgegeben (Auswahl der SSID, Eingabe des Netzwerkschlüssels). Je nach Betriebssystem werden die Verbindungsinformationen gespeichert und müssen bei späteren Verbindungen nicht noch einmal eingegeben werden (Einstellung „automatisch verbinden“, „Zugangsdaten speichern“ o. ä.).
2. Anmeldung am Portal mit den Anmeldedaten des pädagogischen Netzes (*vorname.nachname@FLC.edu.sffm*, „FLC“ ist der „Four-Letter-Code“ der Schule), die Nutzungsbedingungen (s. Abschnitt 8.2) müssen akzeptiert werden. Das Portal erscheint je nach System automatisch oder beim ersten Zugriff auf das Internet (z. B. beim Aufruf des Browsers, ggf. muss dieser neu gestartet oder die Seite aktualisiert werden):



Auch an dieser Stelle bieten einige Systeme an, die Zugangsdaten zu speichern, so dass bei späteren Zugriffen diese nicht noch einmal eingegeben werden müssen. Beachten Sie, dass dadurch – etwa beim Verlust des Gerätes – ein Sicherheitsproblem entstehen kann, da die Zugangsdaten zum pädagogischen Netz in fremde Hände geraten können.

Falls nicht automatisch auf die Anmeldeseite umgeleitet wird (die Verbindung zu einer gewünschten Webseite kann nicht aufgebaut werden, s. Fehlermeldung in Abb. rechts), den vom Browser angebotenen Link (Pfeil) anklicken oder den Browser neu starten.

Hinweis für Grund- und Förderschulen, die im pädagogischen Netz „Tierkonten“ verwenden: Die Anmeldung mit Tierkonten ist im BYOD-WLAN leider nicht möglich. Bitte lassen Sie – falls nicht ohnehin bereits erfolgt – die Anmeldung über den vollen Namen (zusätzlich zu den Tierkonten) beim IT-Service freischalten; schicken Sie dazu eine LUSD-Export-Schülerliste. Für die Festlegung des Passwortes muss die Anmeldung für jedes Namenskonto einmal an einem stationären PC erfolgen.

Nach der Anmeldung können im Browser Internetseiten aufgerufen werden oder Apps gestartet werden.

Nähere Informationen, wie man ein Gerät mit einem WLAN verbindet, erhalten Sie beispielsweise unter:

- Android: https://support.google.com/android/answer/9075847?hl=de
- iOS: https://support.apple.com/de-de/HT202639
- Windows 10: https://support.microsoft.com/de-de/help/4027030/windows-10-connect-to-a-wi-fi-network

Maximal können drei Geräte eines Benutzers/einer Benutzerin angemeldet werden. Bei Anmeldung eines weiteren Gerätes wird die Verbindung mit dem ältesten registrierten Gerät getrennt und eine entsprechende Meldung angezeigt (siehe nebenstehende Abb.).

Die Anmeldung wird gespeichert, so dass bei wiederholter Verbindung mit dem BYOD-Netz die Eingabe der Anmeldedaten meist nicht erforderlich ist. Aufgrund von Datenschutzvorgaben muss die Liste der Anmeldungen jedoch regelmäßig gelöscht werden, so dass von Zeit zu Zeit eine Neuanmeldung verlangt wird. Wird häufig eine Anmeldung verlangt, beachten Sie den Hinweis im Abschnitt 6.5.

5 Gast-WLAN (Hotspot)

5.1 Eigenschaften

Das Gast-WLAN ermöglicht es den Schulen, Gästen (Kooperationspartner, Veranstalter, Veranstaltungsteilnehmer etc.) einen kostenfreien Zugang zum Internet zu gewähren.

Die Authentifizierung im Gast-WLAN erfolgt über ein webbasiertes Portal mittels Benutzername und Passwort. Im Unterschied zu den beiden anderen Netzen ist die Benutzerverwaltung von derjenigen des pädagogischen Netzes unabhängig. Nutzungsberechtigungen für das Gast-WLAN werden einzeln erstellt und sind zeitlich begrenzt. Pro angemeldetem Anwender können maximal drei Endgeräte gleichzeitig mit dem Netz verbunden werden. Zurzeit bestehen keine Beschränkungen des Datenvolumens oder in den Nutzungszeiten. Werden im Verlauf der sukzessiven Hinzunahme weiterer Schulen in den WLAN-Betrieb Engpässe festgestellt, können sich hier ggf. Anpassungen ergeben.

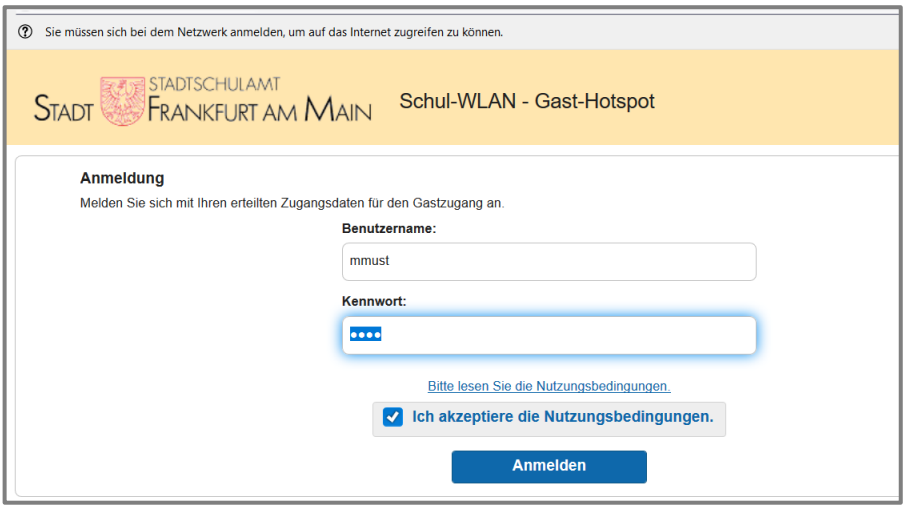
Die Anlage und Pflege der Gast-Netz-Accounts erfolgt durch sogenannte Sponsor-User. Die Rolle des Sponsor-Users ist auf die Mitglieder der Schulleitung sowie die IT-Beauftragten der jeweiligen Schule übertragen worden.

5.2 Verbindungsaufbau

SSID (Netzname):	**Hotspot**
Netzwerkschlüssel:	*wird vom Servicedesk des Stadtschulamtes mitgeteilt, bitte dem Gastnutzer bei Ausstellung des Vouchers übergeben*
Anmeldung:	*am Portal (Anmeldemaske) mit den Daten aus dem Voucher (Benutzername, 4-stelliger Schlüssel)*
Der Netzwerkschlüssel wird jährlich zum Schuljahresbeginn geändert und den IT-Beauftragten vom Servicedesk des Stadtschulamtes mitgeteilt.	

Die Verbindung mit dem Internet geschieht in zwei Stufen.

1. Verbindung mit dem WLAN, wie durch das Betriebssystem des Endgerätes vorgegeben (Auswahl der SSID, Eingabe des Netzwerkschlüssels). Je nach System werden die Verbindungsinformationen gespeichert und müssen bei späteren Verbindungen nicht noch einmal eingegeben werden (Einstellung „automatisch verbinden“, „Zugangsdaten speichern“ o. ä.).
2. Anmeldung am Portal mit den Anmeldedaten aus dem ausgestellten Voucher (Anmeldenamen, 4-stelliger Schlüssel), die Nutzungsbedingungen (s. Abschnitt 8.2) müssen akzeptiert werden. Das Portal erscheint je nach Betriebssystem automatisch oder beim ersten Zugriff auf das Internet (z. B. beim Aufruf des Browsers, ggf. muss dieser neu gestartet oder die Seite aktualisiert werden):



Danach können im Browser Internetseiten aufgerufen werden oder Apps gestartet werden. Der Text der Nutzungsbedingungen ist auf der Anmeldeseite verlinkt und kann vor der Anmeldung eingesehen werden.

Falls nicht automatisch auf die Anmeldeseite umgeleitet wird (die Verbindung zu einer gewünschten Webseite kann nicht aufgebaut werden, s. Fehlermeldung in Abb. rechts), den vom Browser angebotenen Link (Pfeil) anklicken oder den Browser neu starten.

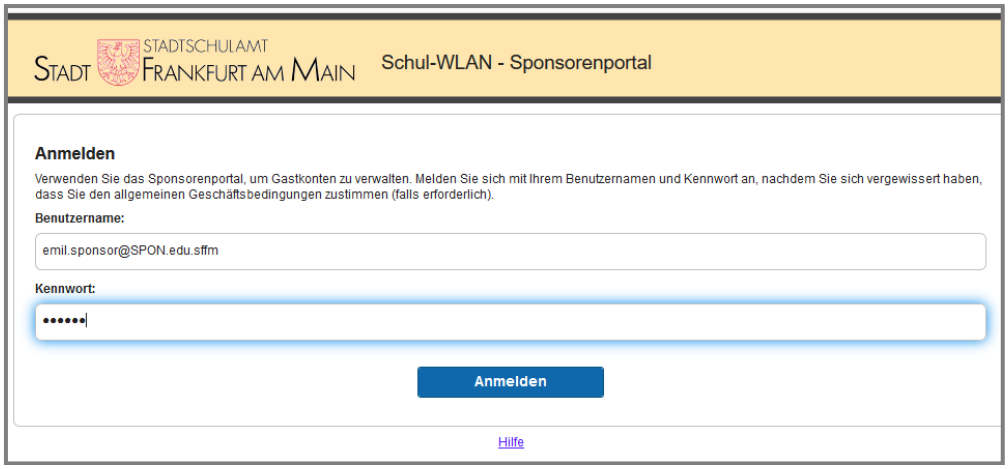
Die Anmeldung wird gespeichert, so dass bei wiederholter Verbindung mit dem Gast-WLAN die Eingabe der Anmeldedaten meist nicht erforderlich ist. Aufgrund von Datenschutzvorgaben muss die Liste der Anmeldungen jedoch regelmäßig gelöscht werden, so dass von Zeit zu Zeit eine Neuanmeldung verlangt wird.

5.3 Einrichtung von Zugangsberechtigungen (Voucher)

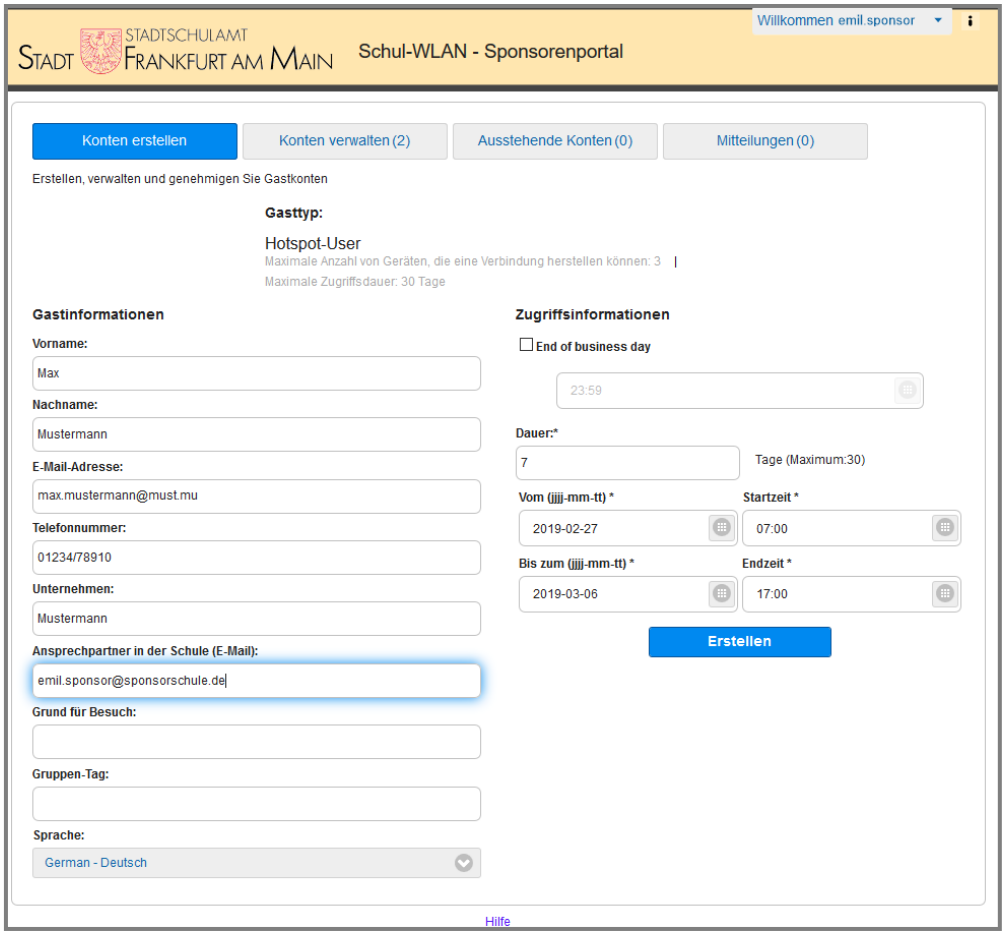
Die Einrichtung von Zugangsberechtigungen für das Gast-WLAN erfolgt über das sog. Sponsorenportal. Dieses erreichen Sie ausschließlich aus dem *pädagogischen* Netz unter der folgenden Adresse:

https://hotspot-edu.stadt-frankfurt.de:8445/sponsorportal/PortalSetup.action?portal=be3d7382-1a34-11e8-9c5e-02423b5391db

Es erscheint zunächst die Anmeldemaske zu diesem Portal:



Die Anmeldung erfolgt mit dem vorhandenen Benutzerkonto des pädagogischen Netzes (*vorname.nachname@FLC.edu.sffm*, „FLC“ ist der „Four-Letter-Code“ der Schule, die Angabe des FLC ist notwendig, ggf. bei den IT-Beauftragten zu erfragen). Ist das angemeldete Konto für die Verwaltung der Gast-Zugänge berechtigt, erscheint nach Bestätigung der Richtlinie die Verwaltungsoberfläche; als Startseite erscheint die Maske für das Anlegen neuer Zugänge („Konten erstellen“):

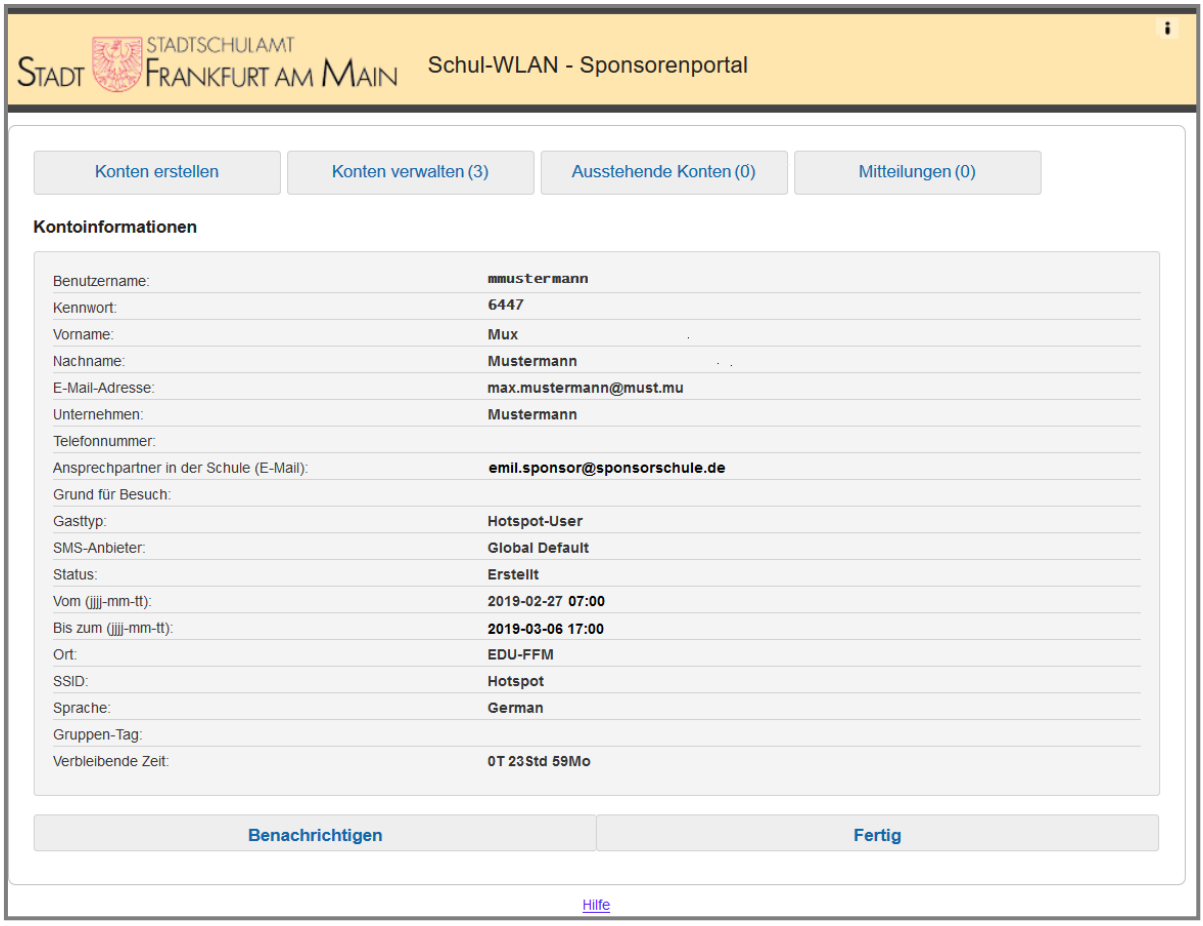


Bitte füllen Sie die folgenden Felder aus:

- **Vorname, Nachname**
  Aus diesen Einträgen wird der Anmeldename generiert (z. B. Max Mustermann → mmustermann). Ohne Angabe dieser Daten wird ein zufälliger (kryptischer) Name erzeugt.
- **E-Mail-Adresse**
  An diese Adresse wird die Mitteilung über die Zugangsdaten versendet. Hier sollte also keine andere E-Mailadresse als die des Gastnutzers stehen. Ohne Angabe müssen die Zugangsdaten auf anderem Wege (z. B. telefonisch oder per Ausdruck) dem Gastnutzer mitgeteilt werden.
- **Ansprechpartner in der Schule**
  Wird hier eine E-Mailadresse eingetragen, erhält der Empfänger eine Mitteilung über die Anlage des Kontos *mit den Zugangsdaten*, dieser kann die Daten dann unabhängig von Ihnen dem Gastnutzer übergeben. Im Normalfall geben Sie hier Ihre eigene E-Mailadresse an.
- **Dauer**
  Anzahl der Tage, die der Voucher gültig sein soll, maximal sind derzeit 30 Tage möglich (Pflichtfeld).
- **Vom / Bis zum / Startzeit / Endzeit**
  Hier können Sie Zeiten eingeben, wenn der Zugang nicht ab sofort bzw. auch zeitlich beschränkt sein soll (z. B. für eine Veranstaltung).

Die Eingabe von Daten in die anderen Felder ist nicht erforderlich bzw. hat in unserer Umgebung keine Bedeutung (z. B. Gruppen-Tag).

Nach Klick auf den Button „Anlegen“ werden die Kontoinformationen zusammenfassend angezeigt:



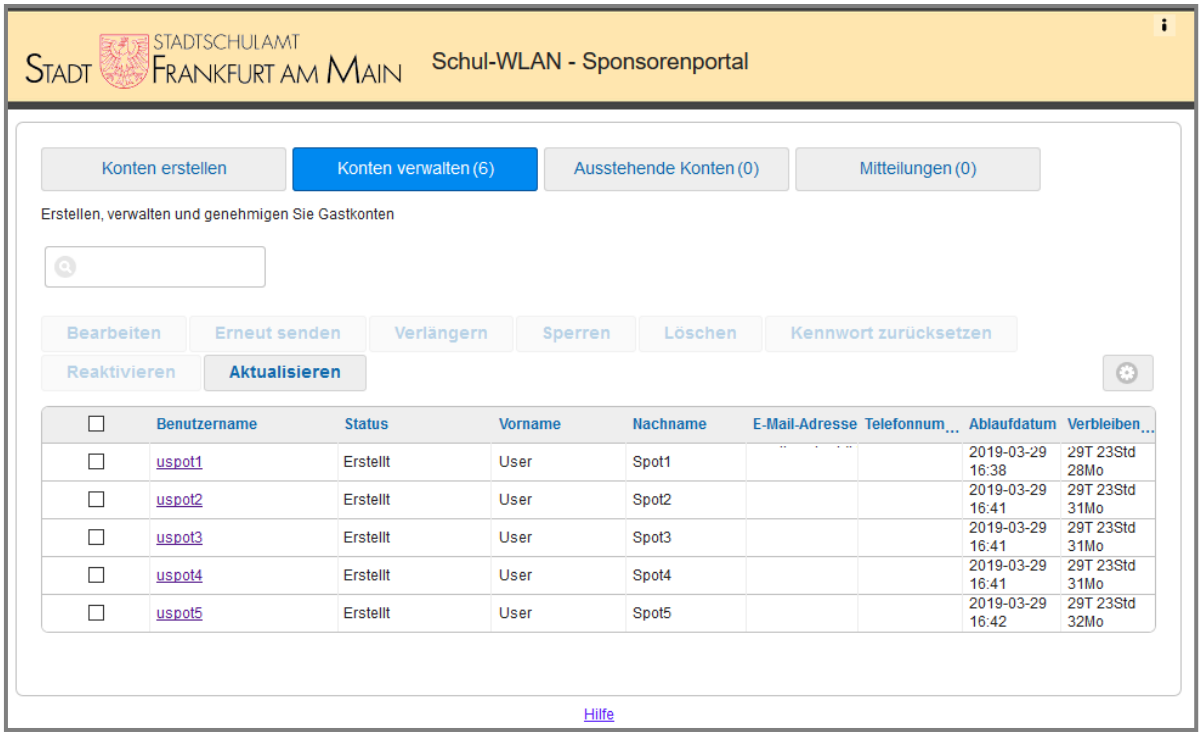
Hier steht auch bereits der generierte 4-stellige Zugangsschlüssel (Kennwort). Mit diesem und dem Benutzernamen kann sich der Gast am Hotspot anmelden. Über den Button „Benachrichtigen“ kann festgelegt werden, wie die Mitteilung der Daten an den Gastnutzer erfolgen soll:

- **Drucken**
  Es erscheint ein Druckdialog, mit dem der Voucher ausgedruckt werden kann. Den Ausdruck übergeben Sie dem Gastnutzer.
- **E-Mail**
  Der Gastnutzer erhält eine E-Mail mit den Zugangsdaten. Über die Option „mich als zusätzlichen Empfänger hinzufügen“ erhalten Sie eine Kopie. Die im Feld „Ansprechpartner in der Schule“ eingegebene Adresse ist hier voreingestellt, kann aber überschrieben werden. Sie ist gleichzeitig die Absenderadresse der Benachrichtigung.

Bitte stellen Sie sicher, dass die Benachrichtigung über die Zugangsdaten nicht an falsche Empfänger gesendet wird und vergessen Sie nicht, dem Gast den Netzwerkschlüssel ebenfalls zu geben.

5.4 Verwalten von Zugangsberechtigungen

Über den Menüpunkt „Konten verwalten“ erhalten Sie eine Übersicht über die von Ihnen angelegten Konten mit den wichtigsten Daten:



Die verschiedenen Funktionen, die für ein oder mehrere ausgewählte Konten aufgerufen werden können (Bearbeiten, Erneut senden, Verlängern, Sperren, Löschen, Kennwort zurücksetzen) sind im Wesentlichen selbsterklärend.

Die Menüpunkte „Ausstehende Konten“ und „Mitteilungen“ haben in unserer Umgebung keine Bedeutung.

Wird das Sponsorportal von einem mobilen Gerät aus aufgerufen, ist die Oberfläche der Bildschirmgröße angepasst, z. B. wird die Maske zur Einrichtung von Konten auf mehrere Seiten verteilt, die Funktionen sind jedoch dieselben (Abb. rechts).

6 Technische Hinweise

6.1 Verwendete Frequenzen und Kanäle

Die Access Points arbeiten sowohl im 2,4- als auch im 5-GHz-Band und nutzen die entsprechend den Normen festgelegten Frequenzen/Kanäle. Da in den Lernzonen i. d. R. Sichtkontakt zum Access-Point besteht, wird mit den schuleigenen pädagogischen Endgeräten (EDU-Netz) das 5-GHz-Band bevorzugt genutzt. So wird ein maximaler Datendurchsatz erreicht. Das 5-GHz-Band wird auch von Radaranlagen benutzt und die WLAN-Steuerung muss die entsprechenden gesetzlichen Einschränkungen (Wartezeiten, Kanalwechsel bei Radarentdeckung) umsetzen. Dies kann im Bereich der Stadt Frankfurt aufgrund der Nähe zum Flughafen relevant sein. Da für das 2,4-GHz- und das 5-GHz-Frequenzband identische WLAN-Funknetznamen (SSID) verwendet werden, ist dies aber für die WLAN-Nutzung ohne Belang.

6.2 Verschlüsselung und Client-Isolation

Alle drei WLAN-Netze arbeiten mit verschlüsselten Verbindungen. Beim BYOD- und Gast-WLAN erfolgt die Verschlüsselung auf Basis des eingegebenen Schlüssels (Pre Shared Key, PSK), im Falle der Geräte des pädagogischen Netzes durch das auf den Geräten hinterlegte digitale Zertifikat. Die PSK werden jährlich zum Schuljahresbeginn gewechselt und den IT-Beauftragten vom Servicedesk des Stadtschulamtes mitgeteilt.

Das Zertifikat besitzt eine zeitlich begrenzte Gültigkeit und muss deshalb regelmäßig über das Netzwerk erneuert werden. Dies ist – neben der Versorgung mit Updates – ein weiterer Grund dafür, dass die mobilen Geräte des pädagogischen Netzes regelmäßig mit dem stationären Netzwerk (z. B. im Notebookwagen) verbunden werden müssen.

Um möglichen Angriffsszenarien vorzubeugen, ist im Bereich des BYOD- und Gast-Netzes die direkte Kommunikation zwischen den WLAN-Endgeräten des jeweiligen Bereiches unterbunden, eine Kommunikation untereinander oder z. B. mit WLAN-Druckern ist nicht möglich (Wireless Client Isolation).

Im EDU-WLAN ist eine Kommunikation untereinander möglich, womit z. B. die Klassen-Management-Software Netop Vision nutzbar wäre.

6.3 Jugendschutzfilter

Da die WLAN-Netze im Schulumfeld betrieben werden, ist allen Verbindungen (also auch dem Gast-WLAN) ein Jugendschutzfilter vorgeschaltet. Eine Deaktivierung ist nicht möglich, schulindividuelle Anpassungen sind wie auch im pädagogischen Netz nicht möglich.

6.4 Protokollbeschränkung

Der Zugang zum Internet im EDU-WLAN ist aus Sicherheitsgründen, wie auch im kabelgebundenen pädagogischen Netz, auf die Protokolle HTTP/HTTPS (Ports 80 und 443) beschränkt. Damit sind Webseitenzugriffe und die Nutzung üblicher Webanwendungen möglich.

6.5 Mindeststandards und Einstellungen für die Geräte

Folgende Mindeststandards müssen von Endgeräten im BYOD- und Gast-Netz erfüllt werden:

- Android: Version 4.4 (KitKat) und nachfolgende
- IOS: Version 7.x und nachfolgende
- Microsoft Windows 7 und nachfolgende
- WLAN-Standard 802.11n, empfohlen WLAN-Standard 802.11ac
- Verschlüsselungsverfahren Wi-Fi Protected Access nach Standard IEEE 802.11i/D9.0 (WPA2-Personal/PSK)

Durch Einhaltung dieser Mindeststandards allein kann jedoch kein einwandfreier Betrieb garantiert werden, da andere Parameter auf den Geräten (Treiber, Gerätekonfiguration) ebenfalls einen Einfluss auf die Funktionalität haben.

Die wiederholte (automatische) Authentifizierung der Geräte im BYOD- und HOTSPOT-Netz erfordert, dass die Geräte anhand ihrer sog. MAC-Adresse wiedererkannt werden können. Normalerweise verwenden Geräte deshalb für einmal gespeicherte WLAN-Netze dieselbe MAC-Adresse, auch wenn eingestellt ist, dass zufällige MAC-Adressen verwendet werden sollen (MAC address randomization, auch als private oder dynamische Adressen bezeichnet). Falls es Probleme mit wiederholter Nutzung des WLANs gibt, z. B. häufige Anmelde-Aufforderungen, sollte diese Einstellung auf feste (Geräte-) MAC-Adresse zurückgesetzt werden. Die Einstellung findet sich im Verbindungs-Dialog unter der jeweiligen SSID im Gerät und ist auch nur für diese gültig. Ihr Gerät verwendet für andere WLANs weiterhin zufällige Adressen.

Deaktivieren Sie am Gerät die Funktion „Private DNS Anfragen“. Auch diese Funktion kann für Verbindungsprobleme verantwortlich sein.

6.6 Möglichkeiten einer Reduzierung der Strahlenbelastung

Es existieren keine belastbaren Beweise für eine gesundheitliche Schädigung durch WLAN-Strahlung. Jedoch unterliegen Schülerinnen und Schüler der Schulpflicht und verbringen viele Stunden im Schulgebäude, woraus sich eine besondere Fürsorge ableitet.

Bei der Auswahl der technischen Infrastruktur wurde größten Wert auf eine möglichst geringe Belastung der Nutzerinnen und Nutzer gelegt. Selbstverständlich halten alle Komponenten die Vorschriften für eine maximale Leistungsabgabe ein. Durch eine automatische Regelung und die Übergabe an den nächstgelegenen Access-Point (Roaming) wird gewährleistet, dass nur die für eine technisch einwandfreie Verbindung nötige Leistung abgestrahlt wird. Werden Verbindungen nur innerhalb einer Lernzone (z. B. eines Klassenraums) benötigt, so regelt der Access-Point die Leistung weitgehend herunter.

Daraus ergibt sich, dass die Strahlenbelastung durch das WLAN auch erheblich von der Nutzung abhängt. Mobilgeräte, die von außerhalb einer Lernzone eine Verbindung anfordern, zwingen u. U. den Access-Point aufgrund der Dämpfung durch Wände die Leistung zu erhöhen. Gestattet die Schule die Nutzung z. B. in Fluren, so kann – muss nicht – eine höhere Strahlenbelastung die Folge sein. Diese bleibt natürlich stets innerhalb der zulässigen Grenzwerte. Abgesehen von der u. U. erhöhten Abstrahlung kann ein belebter Flur mit vielen BYOD-Geräten eine nennenswerte Datenkapazität vom Access-Point abrufen, die dann im Klassenraum nicht zur Verfügung steht.

Für die Belastung durch elektromagnetische Strahlung ist die Summe aller Quellen zu betrachten. Neben dem WLAN sind dies andere, meist private Geräte, die z. T. sogar höhere Leistung abstrahlen oder näher am Körper, insbesondere am Kopf, getragen und verwendet werden. Um proaktiv die Summe der möglichen Strahlenbelastungen zu minimieren, kann eine Schule etwa durch Richtlinien die Nutzung von abstrahlenden Geräten begrenzen. Dazu gehören z. B. Regelungen wie:

- Beschränkung der Nutzung des BYOD-WLANs: Vom gänzlichen Verbot über Nutzung nur durch die Lehrerschaft oder bestimmter Klassen(stufen) bis zur Freigabe nur in bestimmten Räumlichkeiten, Verbot der Nutzung außerhalb der Klassenräume oder bestimmter Aufenthaltsbereiche sind hier viele Varianten denkbar.
- Festlegung einer BYOD-Policy, in der klare Rahmenparameter für den Einsatz eigener Geräte (dazu gehören auch Bluetooth-Hörer o. ä.) durch die Schüler und Schülerinnen geregelt werden. Hierzu können Vorgaben zur (z. B. zeitlichen) Nutzung, eine Liste verbotener Geräte sowie sonstige Nutzungsbeschränkungen gehören.

Solche Regelungen verringern auch die Wahrscheinlichkeit, dass das schulische WLAN gestört wird (s. nächsten Abschnitt).

6.7 Minimierung von Störungen

Störungen des WLAN-Betriebs können von außerhalb und innerhalb des Schulgebäudes kommen. Während man im ersten Fall kaum Möglichkeiten des Schutzes hat, können im Schulgebäude Vorkehrungen getroffen werden, um Störungen möglichst gering zu halten. Störungen von außerhalb sind in erster Linie WLAN-Netze aus der Nachbarschaft. Diesen wird der WLAN-Controller nach Möglichkeit durch Ausweichen auf freie WLAN-Kanäle begegnen. Störungen innerhalb des Schulgebäudes können von einer Vielzahl von Geräten verursacht werden. Als Kandidaten und mögliche Gegenmaßnahmen seien genannt:

- Andere WLAN-Netze: Das können selbst aufgebaute WLANs der Schule oder – sehr viel häufiger – auf Smartphones konfigurierte Hotspots sein. Weisen Sie alle Schulangehörigen und Gäste der Schule, z. B. in einer Haus- oder Nutzungsordnung, darauf hin, dass eigene Hotspots im Schulgebäude nicht zulässig sind. An Schulen mit städtischem WLAN sind lt. Nutzungsvereinbarung mit dem Schulträger andere schulische WLANs nicht gestattet.
- Viele Geräte der Unterhaltungs- und audiovisuellen Technik können in den vom WLAN genutzten Frequenzbändern senden und dadurch das WLAN stören. Beispiele sind Spielkonsolen, Foto-, Web- und Videokameras, Audiokommunikationsgeräte (z. B. Babyfons) u. ä. Halten Sie solche Geräte bei einer gewünschten Nutzung in WLAN-Lernzonen im Blick und untersagen Sie die private Nutzung. Geräte, die im 2,4-GHz-Band senden, können auch in benachbarten Räumen noch stören.
- Bluetooth-Geräte: Drahtlose Kopfhörer und Lautsprecher, Funkmäuse u. v. a. Bluetooth hat zwar eine geringe Reichweite und „weicht“ detektierten WLAN-Funkkanälen aus, insbesondere bei einer größeren Anzahl von Geräten, z. B. in einem Klassenraum, sind jedoch Störungen wahrscheinlich. Schülerinnen und Schüler sollten daher in Lernzonen keine Bluetooth-Geräte nutzen.
- Eher unwahrscheinlich aber möglich sind Störungen durch weitere Geräte wie Mikrowellengeräte (bei unmittelbarer Nachbarschaft zu einem Access-Point), nicht für den mitteleuropäischen Raum

zugelassene DECT-Telefone und defekte oder nicht korrekt geschirmte Geräte (z. B. in einem Elektroniklabor).

Insbesondere, wenn Probleme bei der Nutzung des WLANs gehäuft in einem bestimmten Teil des Schulgebäudes auftreten, ist an störende Geräte zu denken.

6.8 Die Infrastruktur (ein Blick hinter die Kulissen)

Um die Dienste der WLAN-Netze zu gewährleisten, wird im Hintergrund eine zentrale und hochverfügbare WLAN-Controller-Infrastruktur betrieben, über welche sämtliche Access-Points des pädagogischen Netzes gesteuert werden. Durch einen hohen Grad an Automatisierung wird zudem ein geringer Personalaufwand erreicht. Die Access-Points werden mit allen nötigen Einstellungen, Sicherheitsregeln, Zertifikaten, Firmware-Updates etc. versehen. Auftretende Fehler werden an zentraler Stelle angezeigt und können von der Administration analysiert und meist ohne Vor-Ort-Einsatz behoben werden. Für die Verteilung der Zertifikate, die Authentifizierungsportale und die Zuweisung der Voucher für das Gast-WLAN dient ein umfassendes Zugriffskontrollsystem (Identity-Management). Die gesamte Infrastruktur wird redundant vorgehalten, so dass eine hohe Ausfallsicherheit gewährleistet ist. Zudem läuft in den lokalen pädagogischen Netzen der Schulen ein Fall-Back-Dienst, der die Schul-interne EDU-WLAN-Funktionalität im pädagogischen Netz auch bei Ausfall der Anbindung (und damit Unterbrechung der Verbindung der Access-Points zum zentralen WLAN-Controller) aufrechterhält. Dadurch kann weiter per WLAN auf das pädagogische Netz (Anmeldung, Netzwerklaufwerke, Drucker) zugegriffen werden. Lediglich die Internet-Verbindung ist dann nicht gegeben. Naturgemäß stehen dann auch das BYOD- und das Gast-WLAN nicht zur Verfügung. Die Authentifizierung der Anwender im BYOD-WLAN erfolgt auf Basis der im Active Directory des pädagogischen Netzes hinterlegten Benutzerkonten.

7 Selbsthilfe und Hinweise zum Support

Bei Problemen mit der Nutzung der WLANs prüfen Sie bitte anhand der Checkliste auf der folgenden Seite einige Punkte, bevor Sie den technischen Support kontaktieren. Voraussetzung ist ein „funktionierendes“ Endgerät, also eingeschaltete WLAN-Funktion und korrekt installierter und konfigurierter WLAN-Treiber; s. a. Abschnitt 6.5.

Ist diese Erstanalyse nicht erfolgreich, geben Sie bitte eine Störungsmeldung auf. Geben Sie dabei dem Support soweit möglich die folgenden Informationen mit:

- Gebäude/Raum-Nr. (Lernzone)
- gestörtes Netz (SSID)
- Zustand des Access-Points (LED-Status)
- Endgerätetyp
- Gerätename bei Geräten des pädagogischen Netzes
- MAC-Adresse bei privaten Geräten
- wird die SSID ausgestrahlt (am Endgerät sichtbar)?
- erfolgt im BYOD- bzw. Gast-WLAN die Umleitung auf das Anmeldeportal?
- verwendetes Zugangskonto
- sonstige Fehlerbeschreibung
- Zeitpunkt des Auftretens der Störung (für das Auffinden von Fehlermeldungen im zentralen WLAN-Management)

	Symptom/Check	mögliche Ursache	Störungsbehebung	Hinweise
1	WLAN-SSIDs („EDU“, „BYOD“, „Hotspot“) werden nicht oder nur schlecht empfangen.	Das Gerät befindet sich nicht in einer Lernzone.	Suchen Sie eine Lernzone auf (Access-Point in *Sichtweite*).	Viele Geräte listen die SSIDs in absteigender Empfangsstärke auf; diese 3 SSIDs sollten in der Liste ganz oben stehen.
2	WLAN-SSIDs („EDU“, „BYOD“, „Hotspot“) werden in einer Lernzone (Access-Point in Sichtweite) nicht empfangen; *auch andere mobile Geräte zeigen diese nicht an*.	Access-Point (AP) sendet nicht.	Status AP-LED: - leuchtet nicht: Verbindung zur Datendose prüfen - blinkt (verschiedene Farben): 15 Min. warten, wenn keine Änderung, AP-Verbindung zur Wanddose trennen und wieder verbinden, erneut 15 Min. warten bis LED grün oder blau stehend leuchtet	Wenn kein Erfolg, Störungsmeldung aufgeben. Wartezeit ist erforderlich, da AP evtl. Neukonfiguration oder Bootvorgang durchführt. Normalzustand ist stehend grün oder blau leuchtende LED.
3	Verbindung mit ausreichend empfangenem WLAN (BYOD, Hotspot) nicht möglich.	Falscher Netzwerkschlüssel.	Netzwerkschlüssel bei IT-Beauftragten erfragen	Schlüssel ändert sich zu Beginn des Schuljahres. Unterschiedliche Netzwerkschlüssel für BYOD und Hotspot.
4	Anmeldung mit Account am Portal nicht möglich (falsches Login)	Falsches Netz	Mit richtigem Netz (BYOD, Hotspot) verbinden.	Das EDU-WLAN kann nicht mit privaten Geräten verwendet werden.
5	BYOD: Anmeldung mit Account am Portal nicht möglich (falsches Login).	Account-Daten (vorname.nachname@FLC.edu.sffm) nicht richtig eingegeben.	Account-Daten richtig eingeben.	Bei der WLAN-Anmeldung ist die Angabe des FLC (s. 4.2) zwingend erforderlich.
6	BYOD: Anmeldung mit Account am Portal nicht möglich (falsches Login). *Login ist auch an einem stationären PC nicht möglich*.	Account im päd. Netz ungültig, weil z. B. gesperrt oder Passwort falsch.	Account im päd. Netz durch IT-Beauftragte/n freigeben/Passwort zurücksetzen lassen.	Eine erzwungene Passwort-Änderung nach Erstanmeldung/Rücksetzung muss auf einem stationären Gerät erfolgen.
7	Hotspot: Anmeldung mit Account am Portal nicht möglich (falsches Login)	Account abgelaufen.	Gast-Account (Voucher) verlängern lassen.	
8	BYOD oder Hotspot: Portal zur Anmeldung wird nicht angezeigt	Verbindung mit dem WLAN noch nicht erfolgt	Verbindung mit richtigem WLAN (SSID „BYOD“ oder „Hotspot“) herstellen.	
		Verbindung ist erfolgt, keine Anmeldemaske	Browser am Gerät neu starten.	
9	BYOD oder Hotspot: Häufige Anmeldeaufforderungen oder Verbindungsprobleme	Geräte-Authentifizierung wird nicht wiedererkannt	Siehe Hinweise im Abschnitt 6.5.	
10	Verbindung eines schuleigenen Gerätes mit dem EDU-WLAN erfolgt in einer Lernzone nicht.	Geräte-Zertifikat ist abgelaufen.	Gerät per Kabel mit einer Datendose des pädagogischen Netzes verbinden (z. B. im Notebookwagen) und neu starten. Geräte regelmäßig (jede Woche) mit dem päd. Netz verbinden.	Das Geräte-Zertifikat verliert seine Gültigkeit, wenn ein Gerät länger nicht mit dem päd. Netz verbunden war.
11	Trotz angezeigter gültiger Verbindung eines schuleigenen Gerätes mit dem EDU-WLAN ist kein Zugriff auf pädagogische Ressourcen oder das Internet möglich.	Verbindung „hängt“.	WLAN-Netz an dem Gerät (angezeigt als EDU-GPO) kurz trennen und wieder verbinden (mit SSID EDU).	Einstellungsdialog über Antippen des WLAN-Symbols in der Taskleiste.
		Anmeldung erfolgte lokal, nicht mit einem pädagogischen Account.	Mit einem Account des pädagogischen Netzes am Gerät anmelden.	
12	Auf einem schuleigenen Gerät wird die SSID des EDU-WLANs als EDU, nicht als EDU-GPO angezeigt	Die Verbindung mit dem EDU-WLAN konnte nicht hergestellt werden.	Siehe Punkte 1 und 10.	

Als allgemeinbildende Schule wenden Sie sich bei Störungen des WLAN-Betriebs wie gewohnt an den Support-Dienstleister für die allgemeinbildenden Schulen, dieser kann auch bei der Erstdiagnose helfen.

Der Servicedesk wird Ihnen in den meisten Fällen ein WLAN-Störungsformular zusenden, das Sie bitte ausfüllen und zurücksenden.

Fehlermeldungen und Anfragen, die mit der Nutzung des WLANs außerhalb der definierten Lernzonen im Zusammenhang stehen, sind vom Support nicht abgedeckt.

Für die privaten Endgeräte im BYOD- oder Gast-WLAN wird kein Support geleistet, der Support beschränkt sich auf die reine Verfügbarkeit dieser Netze (wenn z. B. mehrere verschiedene Geräte keine Verbindung herstellen können).

8 Rechtliches

8.1 Zuständigkeit

Die Zugänge zu den WLAN-Netzen werden durch die Schule verwaltet – entweder über die Konten des pädagogischen Netzes im Falle des EDU- und BYOD-WLANs oder die Voucher im Falle des Gast-WLANs. Daraus ergibt sich die grundsätzliche Verantwortlichkeit der Schule für die Nutzung dieser Netze, wie sie bereits für das pädagogische Netz besteht. Im Falle von nicht-technischen Anfragen oder Eingaben der Nutzer und Nutzerinnen oder von Dritten (z. B. Rechteinhabern) empfehlen wir die Einbindung des staatlichen Schulamtes. Das Stadtschulamt bzw. das Amt für Informations- und Kommunikationstechnik sind grundsätzlich nur für den technischen Betrieb zuständig.

8.2 Nutzungsvereinbarungen und Datenschutz

Da Nutzer des EDU- und BYOD-WLANs stets auch Nutzer des pädagogischen Netzes der Schule sind, haben diese mit der aktuellen Nutzungsvereinbarung der Schule zum pädagogischen Netz (bei Verwendung der Mustervorlage des Stadtschulamtes) die Regeln zur Nutzung des WLANs anerkannt.

Gastnutzer müssen beim Aufbau der Verbindung mit dem Gast-WLAN auf der Anmeldemaske die Annahme einer hinterlegten Nutzungsvereinbarung bestätigen.

Beide Nutzungsvereinbarungen enthalten eine Datenschutzerklärung und eine Einverständniserklärung zur Verarbeitung von personenbezogenen Daten, die für den Betrieb der Netze nötig sind.

Die Schule kann die Nutzungsvereinbarung durch eine BYOD-Policy ergänzen, in der klare Rahmenparameter für den Einsatz eigener Geräte durch die Schüler und Schülerinnen geregelt werden. Hierzu können Vorgaben zur (z. B. zeitlichen) Nutzung, eine Liste verbotener Geräte sowie sonstige Nutzungsbeschränkungen gehören.

Hinsichtlich der Aufsicht gelten die Regelungen des Hessischen Schulgesetzes auch für die Verwendung von WLAN-Endgeräten.

Werden die nutzereigenen Geräte im Unterricht benutzt (BYOD), ist auf den Schutz der privaten Daten auf den Geräten der Nutzer zu achten. Jugendliche müssen der Aufsichtsperson nur auf freiwilliger Basis ihr privates Endgerät vorzeigen.

Bei stichprobenartigen Endgerätekontrollen im Rahmen der Aufsichtspflicht ist zu berücksichtigen, dass die privaten Geräte im Regelfall auch private Daten der Schüler und Schülerinnen enthalten. Ein Zugriff auf diese Daten durch Lehr- und Aufsichtspersonal ist grundsätzlich, auch im Falle des Verdachts von Zugangsmissbrauch, ohne gültiges Einverständnis (also ggf. der Erziehungsberechtigten) unzulässig. So dürfen insbesondere keine privaten E-Mails, Fotos, Tonaufzeichnungen oder ähnliche Daten durch den Lehrer oder die Lehrerin eingesehen werden.

Allerdings müssen es Schüler und Schülerinnen unter Umständen dulden, dass eine Lehrkraft das private Endgerät einzieht. Hier hängt es davon ab, was die jeweilige Schulordnung/BYOD-Policy vorschreibt. Normalerweise muss die Lehrkraft das Handy aber wieder zurückgeben, sobald es nicht mehr stört.

Diese Hinweise entstanden im Rahmen der Betrachtung der rechtlichen Aspekte einer Einführung von WLAN an Schulen. Sie haben keinen rechtsverbindlichen oder beratenden Charakter. Generell sind in diesen Fragen die Schulaufsicht/das Staatliche Schulamt und der schulische Datenschutzbeauftragte zuständig.