

Ausstattungsprogramm „Schulische iPads“

Häufig gestellte Fragen (FAQs)



hello

IT-Sicherheit und Datenschutz

Wie bildet der Schulträger die Sicherheit der eingesetzten iPads ab?

Die iPads werden beim Schulträger durch ein MDM-System* zentral verwaltet. Das bedeutet, dass die Geräte eine für den sicheren pädagogischen Einsatzzweck geeignete Konfiguration erhalten, bei Verlust oder Diebstahl gelöscht und geortet werden können und bestimmte Gerätefunktionen (z.B. AppStore-Käufe, Besuch bestimmter Webseiten) eingeschränkt werden kann.

Die Verwaltung der iPads ist dauerhaft aktiv, d.h. auch in privaten WLAN-Umgebungen sind die Geräte geschützt.

In der Schule werden die iPads in einem speziellen pädagogischen Netzwerk eingesetzt, welches eine mehrstufige Sicherheitsarchitektur aus Firewall, Webfiltern und Virenschutz aufweist.

Unter Beteiligung der der schulischen Datenschutzbeauftragten wurde eine DSGVO-konforme Lösung zum Umgang mit der schulischen Infrastruktur und den Daten auf den iPads entwickelt.

* MDM = Mobile Device Management-System
eine Softwarelösung zur Fernverwaltung von mobilen Endgeräten an Schulen

Wie wird der Datenschutz gewährleistet?

Der Schulträger hat eine individuelle Vereinbarung zur Auftragsdatenverarbeitung mit der Firma Apple abgeschlossen und diese mit den schulischen Datenschutzbeauftragten abgestimmt. Kernelemente für die DSGVO-Konformität der Lösung sind u.a. eine Ende-zu-Ende-Verschlüsselung, Zwei-Faktor-Authentifizierung sowie der Einsatz anonymisierter „Managed-Apple-IDs“.

Zudem ist die MDM*-Architektur so aufgebaut („Security by Design“), dass es dem Schulträger nicht möglich ist, auf Grund der Seriennummer des iPads Rückschlüsse auf den oder die Schüler*in zu treffen – die Zuordnung „Gerät – Schüler*in“ ist nur der Schule selbst bekannt.

Können Schüler*innen durch die zentrale Verwaltung der Geräte „überwacht“ werden?

Es besteht zu keiner Zeit durch den Schulträger die Möglichkeit, aktiv auf Kamera, Mikrofon, Daten oder GPS-Lokation des Gerätes zuzugreifen.

Im Fall eines gemeldeten Verlusts oder Diebstahl wird das Gerät in einen speziellen „Lost-Modus“ geschaltet und ist dann nicht mehr nutzbar – erst dann ist eine Fernlöschung oder Ortung des Gerätes möglich.

