Otto-Nagel-Gymnasium

Otto-Nagel-Gymnasium - Schulstraße 11 - 12683 Berlin
Tel: +4930 514 38 64 - Fax: +4930 514 28 16
http://www.ong.berlin
sekretariat@ong.berlin

BERLIN

Berlin, den 25.02.2025

Mindestsicherheitsstandards

Beim Einsatz der dienstlichen Geräte sind die nachfolgend aufgeführten Mindestsicherheitsstandards zu beachten, um sicherzustellen, dass

- dienstliche Daten vertraulich behandelt werden und
- dienstliche Daten besonders geschützt sind.

1. Nutzung eines sicheren Endgeräts und eines sicheren Betriebssystems

Voraussetzung für ein sicheres Endgerät ist, dass Sicherheitseinstellungen beachtet und die Betriebssysteme sowie Programme regelmäßig aktualisiert werden. Aktuelle Betriebssysteme, die vom jeweiligen Anbieter gepflegt werden, können als sicher betrachtet werden, solange die Sicherheitseinstellungen (vgl. BSI) beachtet bzw. nicht bewusst deaktiviert werden.

2. Sichere Softwareauswahl/-einsatz

2.1 Installation der Software

Es ist gestattet, Software aus dem zur Verfügung gestellten schulinternen App-Store (Jamf Teacher) zu installieren. Die Installation von Software aus anderen Quellen ist untersagt.

2.2 Software zur Verarbeitung personenbezogener Daten

Vor der Nutzung einer Software, durch die personenbezogene Daten verarbeitet werden, hat eine Freigabe durch die Schulleitung oder der durch die Schulleitung bevollmächtigten Personen (Datenschutzbeauftragte) zu erfolgen.

3. Betrieb des Endgeräts in einer sicheren Netzwerkumgebung

In einem schulischen Netzwerk mit Zugangsbeschränkungen, kann davon ausgegangen werden, dass das Netzwerk sicher ist und aus dem Netzwerk heraus keine Angriffe auf ein Endgerät erfolgen. Entsprechendes gilt auch für das Heimnetzwerk, wenn man ein sicheres WLAN-Passwort gesetzt und am Heimrouter keine Verbindungen von außen ins Heimnetz geöffnet hat. Einschränkungen gelten gegebenenfalls, wenn unzureichend abgesicherte Smart-Home-Geräte im Heimnetz betrieben werden, die von sich aus eine Internetverbindung öffnen.

Betrieb des Endgeräts in unterschiedlichen Umgebungen

Wenn dienstliche Endgeräte in unterschiedlichen Umgebungen (z. B. öffentliches WLAN) genutzt werden, fehlt der Schutz der schulischen oder häuslichen Umgebung und des lokalen Netzwerks. Deshalb muss in besonderer Weise sichergestellt sein, dass

- das Endgerät vor unberechtigten physischen Zugriffen geschützt ist und
- das Endgerät vor Angriffen bzw. unberechtigten Zugriffen aus dem lokalen Netzwerk und aus dem Internet geschützt ist.

4. Zugriff auf das Endgerät nur durch die jeweilige Lehrkraft

Der Zugriff auf das Endgerät darf nur durch die jeweilige Lehrkraft erfolgen. Ist die Nutzerin bzw. der Nutzer an einem Endgerät mit persönlichen Zugangsdaten angemeldet (z. B. mit Benutzernamen und starkem Passwort), ist der Zugriff von fremden Personen zumindest erschwert. Beim Verlassen des Arbeitsplatzes sollte sich die Lehrkraft abmelden oder das Endgerät sperren (z.B. Bildschirm zuklappen). Bei zu langer Inaktivität kann auch eine automatische Sperrung des Endgeräts erfolgen.

5. Verschlüsselte Ablage von dienstlichen Daten

Die verschlüsselte Ablage von Dateien oder Dokumenten bietet auch dann noch Schutz, wenn diese in die falschen Hände geraten. Bei der Verschlüsselung von Daten steht die Vertraulichkeit im Vordergrund. Es soll gewährleistet sein, dass ohne den zugehörigen Schlüssel bzw. ohne das Passwort die Dokumente nicht lesbar sind. Der zugehörige Schlüssel muss an einem sicheren Ort aufbewahrt werden.

Möglich ist die Verschlüsselung einzelner Dokumente, die Ablage der Dokumente in verschlüsselten Containern oder die Verschlüsselung ganzer Partitionen bzw. Dateisysteme.

6. Speicherfristen

Die gesetzlichen Aufbewahrungsfristen sind einzuhalten z.B. das Löschen von digitalen Notenlisten nach Zweckverfall (üblicherweise am Ende eines Schuljahres).

7. Backup der dienstlichen Daten

Sofern ein Backup erstellt wird, muss auf den Zugriffsschutz und auf eine Verschlüsselung geachtet werden. Um einem Verlust der Daten vorzubeugen, empfiehlt es sich, regelmäßig Sicherungskopien der wichtigen Daten anzufertigen und diese an einem sicheren Ort aufzubewahren. Bei Backups sind ebenfalls die unter Ziffer 6 genannten Aufbewahrungsfristen einzuhalten. Eine Datensicherungen via Clouddienste sind nur mit den von der Schule zur Verfügung gestellten Systemen zulässig (OneDrive, SynologyDrive).