

**Betreff:** Wichtiger Hinweis zum sicheren Umgang mit persönlichen WLAN-Zugangsdaten

Liebe Eltern, liebe Schülerinnen und Schüler,

unsere Schule stellt allen Schülerinnen und Schülern den Zugang zum schulischen WLAN (WGM Radius) über **persönliche Zugangsdaten von IServ** zur Verfügung. Diese Daten sind mit dem **IServ-Benutzerkonto verknüpft** und ermöglichen den Zugang zum Internet auf dem Schulgelände.

Wir möchten an dieser Stelle eindringlich darauf hinweisen, wie wichtig ein **verantwortungsvoller und sicherer Umgang** mit diesen Zugangsdaten ist:

1. **Zugangsdaten sind streng persönlich.** Sie dürfen **unter keinen Umständen** an andere Personen weitergegeben werden – auch nicht an Freunde oder Mitschüler.
2. **Sicherheit geht vor.**
  - Zugangsdaten sollten niemals für andere sichtbar aufgeschrieben oder ungeschützt gespeichert werden.
  - Bei Verdacht, dass jemand anderes die eigenen Zugangsdaten kennt, muss **sofort das Passwort über IServ geändert** werden.
3. **Missbrauch hat Konsequenzen.** Der Login über die Zugangsdatendaten wird protokolliert und ist dem jeweiligen Benutzer eindeutig zuzuordnen. Das bedeutet:
  - Bei einem Missbrauch (z. B. Aufruf verbotener Inhalte, Cybermobbing, illegale Downloads, beleidigende Nachrichten) ist **immer der Inhaber des Benutzerkontos verantwortlich** – unabhängig davon, wer tatsächlich das Gerät genutzt hat. Entsprechend muss der/die Kontoinhaber:in auch mit pädagogischen und ggf. rechtlichen Konsequenzen rechnen.

Der sichere Umgang mit den Zugangsdaten schützt Ihre Kinder nicht nur vor Konsequenzen, sondern auch die persönliche Privatsphäre und die Sicherheit unseres gesamten Schulnetzwerks.

Bitte besprechen Sie das Thema mit Ihrem Kind und bestätigen den Erhalt des Schreibens.

Mit freundlichen Grüßen

