

NUTZUNGSORDNUNG für den Einsatz von WebUntis

Der Funktionsumfang und die Bestandteile von WebUntis sind im Einzelnen im Benutzerhandbuch des Herstellers in der jeweils aktuellen Fassung beschrieben.



Zulässiger Datenumfang

Daten der Schüler • Grunddaten: Familienname, Rufname, Vorname, Namensbestandteile, Kurzname, Geschlecht, Geburtsdatum, Ordnungsnummer (nicht einsehbar, rein technische Speicherung).

Aktuelle Unterrichtsdaten: Schule, Schulart, Klasse, Jahrgangsstufe, Klassenart, Unterrichtsart

Allgemeine Hinweise zum Umgang mit Kennwörtern

- Halten Sie das Kennwort geheim und geben Sie es nie weiter.
- Ändern Sie das Kennwort regelmäßig.
- Schreiben Sie das Kennwort nach Möglichkeit nicht auf bzw. verwahren Sie aufgeschriebene Kennwörter sicher.
- Speichern Sie das Kennwort nicht unverschlüsselt ab.
- Verwenden Sie für dienstliche und private Zwecke unterschiedliche Kennwörter.
- Ändern Sie das Kennwort, falls der Verdacht besteht es könnte jemand anderem bekannt sein.
- Verwenden Sie sichere Kennwörter

Zugangsdaten

- Der Benutzer ist verpflichtet, die eigenen Zugangsdaten zum WebUntis-Konto geheim zu halten. Sie dürfen nicht an andere Personen weitergegeben werden.
- Sollte der Verdacht bestehen, dass die eigenen Zugangsdaten anderen Personen bekannt geworden sind, ist der Benutzer verpflichtet, sofort Maßnahmen zum Schutz der eigenen Zugänge zu ergreifen. Falls noch möglich, sind Zugangspasswörter zu ändern. Ist dieses nicht möglich, ist ein schulischer Administrator zu informieren.
- Sollte der Benutzer in Kenntnis fremder Zugangsdaten gelangen, so ist es untersagt, sich damit Zugang zum fremden Benutzerkonto zu verschaffen. Der Benutzer ist jedoch verpflichtet, den Eigentümer der Zugangsdaten oder einen schulischen Administrator zu informieren.
- Nach Ende der Unterrichtsstunde oder der Arbeitssitzung an einem schulischen Rechner bzw. Mobilgerät meldet sich der Benutzer von WebUntis ab (ausloggen).

Datenschutz- und IT-Sicherheitsvorfälle

Bei Verdacht der Gefährdung der IT-Sicherheit und bei IT-Sicherheitsvorfällen ist der zuständige Administrator oder der IT-Sicherheitsbeauftragte der Neuen Oberschule zu verständigen. Im Umgang mit Sicherheitsvorfällen sind Ehrlichkeit und Kooperationsbereitschaft besonders wichtig. Die Meldung von Sicherheitsvorfällen wird positiv gewürdigt. Bei datenschutzrelevanten Vorfällen ist zusätzlich der behördliche Datenschutz zu informieren

Zur Kenntnis genommen

Name des Schülers / der Schülerin:

Datum, Unterschriften der Nutzenden (Schülerin / Schüler und Eltern)