



### *PC-Arbeitsstationen, Tablets und sonstige Hardware*

---

- Es ist jede Aktivität zu vermeiden, die die Arbeitsstationen beschädigt oder funktionsuntüchtig macht.
- Das Mitbringen und Einnehmen von Speisen und Getränken in den Fachräumen und der Mediothek ist nicht gestattet.
- Veränderungen an der Konfiguration und den Installationen sowie Manipulationen an der Hardwareausstattung sind untersagt.
- Die Nutzung des Unterrichtsnetzes und das Anmelden an Arbeitsstationen ist nur Berechtigten und diesen nur mit ihren persönlichen (passwortgeschützten) Benutzerkürzeln gestattet.
- Für Handlungen, die unter seiner/ihrer Nutzerkennung erfolgt sind, wird der Schüler/die Schülerin ggf. verantwortlich gemacht. Deshalb muss das Passwort vertraulich gehalten werden. Das Arbeiten mit einem fremden Zugang ist verboten.
- Für jede/n Benutzer/in wurde ein "persönlicher Arbeitsordner" eingerichtet, der ausschließlich diesem/dieser Benutzer/in zur Verfügung steht. Außer in diesem Arbeitsordner darf kein anderer Ordner des Netzwerks zu Speicherungen benutzt werden. In diesem Arbeitsordner dürfen sich nur solche Daten befinden, die im Unterricht erstellt bzw. vom Fachlehrer/von der Fachlehrerin zur Verfügung gestellt worden sind.
- Jeder/jede Benutzer/in ist für alle Aktivitäten während seiner/ihren Arbeitssitzungen voll verantwortlich und trägt ggf. die rechtlichen Konsequenzen.
- Jeder/jede Benutzer/in muss nach seiner/ihrer Arbeitssitzung die Arbeitsstation ordnungsgemäß herunterfahren.
- Das Aufrufen oder Herunterladen von Seiten oder Dateien mit rechtsradikalen, rassistischen, kriminellen oder pornografischen Inhalten verstößt gegen geltendes Recht und ist untersagt.
- Das Herunterladen von Musikdateien, Filmen oder Software ist ausschließlich zu Unterrichtszwecken und nach vorheriger Genehmigung durch den / die Fachlehrer / Fachlehrerin erlaubt.
- Das Benutzen von Chat, Messenger und derartigen Webdiensten bzw. Seiten ist nicht gestattet.
- Zuwiderhandlungen gegen diese Benutzerordnung können neben dem Entzug der Nutzungsberechtigung weitere disziplinarische Maßnahmen nach sich ziehen.
- Vorsätzlich herbeigeführte Zerstörungen oder Beschädigungen an Hard- und Software führen in jedem Falle zur Geltendmachung von Schadenersatzansprüchen durch die Schulleitung. Darüber hinaus sind Disziplinarmaßnahmen vorbehalten.
- Der Internet-Zugang soll grundsätzlich nur für Zwecke genutzt werden, die mit Ihrer Ausbildung zusammenhängen.
- Für die langfristige Sicherung der erstellten Dateien ist jeder/ jede Benutzer/in selbst verantwortlich. Alle Dateien werden jedes Schuljahr vor den Sommerferien gelöscht und eine Systemwiederherstellung durchgeführt – bei diesem Prozess gehen alle Daten verloren.

### 1. Gestattung des Internetzuganges

Die BBS3 Oldenburg ermöglicht Endnutzerinnen und Endnutzern im Rahmen des schulischen WLANs den Internetzugang. Der Endnutzer/die Endnutzerin ist zur Nutzung des Internetzuganges berechtigt, wenn er/sie bzw. seine gesetzlichen Vertreter diese Nutzungsbedingungen akzeptieren und er/sie sich mit gültigen Zugangsdaten eingeloggt hat. Es besteht kein Anspruch auf Nutzung des Internetzuganges. Diese Nutzungsordnung regelt die Voraussetzungen, unter denen die Nutzung des schulischen WLAN technisch zur Verfügung stellt.

### 2. Verfügbarkeit

Es wird ausdrücklich darauf hingewiesen, dass die Schule die Möglichkeit hat, Jugendschutzmaßnahmen zu ergreifen und den Zugriff auf Inhalte zu filtern. Für die Nutzung des WLAN ist ein zu IEEE 802.11n oder höher<sup>1</sup> kompatibles Endgerät erforderlich. Es werden weder Mindestbandbreite noch Störungsfreiheit garantiert.

### 3. Verantwortung, Gefahren

Die BBS3 Oldenburg ist nicht für Inhalte verantwortlich, die von der Endnutzerin/dem Endnutzer oder Dritten über das WLAN abgerufen, in das Internet eingestellt oder in irgendeiner Weise verbreitet werden. Die Nutzung des Internetzuganges erfolgt auf eigene Gefahr und auf Risiko der Endnutzerin/des Endnutzers. Die Störerhaftung geht insoweit auf die Endnutzerin/den Endnutzer über. Die Datenübertragung erfolgt ohne Verschlüsselung. Bei Bedarf muss die Endnutzerin/der Endnutzer eigene Maßnahmen zur Sicherung seines Datenverkehrs ergreifen.

### 4. Pflichten der Endnutzer

Der Endnutzer/die Endnutzerin darf das WLAN nur bestimmungsgemäß und nach Maßgabe der in der Bundesrepublik Deutschland geltenden Gesetze und Verordnungen benutzen. Der Endnutzer/die Endnutzerin ist verpflichtet, die angebotenen Telekommunikationsdienstleistungen bei Nutzung des WLANs nicht zu Zwecken zu missbrauchen, die den gesetzlichen Bestimmungen oder diesen Endnutzerbedingungen widersprechen.

Das bedeutet:

Es ist verboten, pornographische, gewaltverherrlichende oder rassistische Inhalte aufzurufen oder zu versenden. Werden solche Inhalte versehentlich aufgerufen, ist die Anwendung zu schließen. Der Endnutzer/die Endnutzerin hat es im Einzelnen zu unterlassen,

- bei der Nutzung des WLANs Straftaten zu begehen und / oder vorzubereiten,
- durch Vervielfältigen und öffentlich zugänglich Machen gegen Urheberrecht zu verstoßen

---

<sup>1</sup> Dies ist ein Standard für drahtlose Netzwerke (WLANs). Der Standard definiert eine Technik zum Aufbau drahtloser lokaler Netzwerke

- Informationen zu verbreiten,
  - die gem. §§ 130, 130a und 131 StGB der Volksverhetzung dienen, und / oder
  - die im Sinne des § 184 StGB pornografisch sind, und / oder
  - die im Sinne der §§ 184 bff StGB geeignet sind, Kinder oder Jugendliche sittlich schwer zu gefährden und / oder in ihrem Wohl zu beeinträchtigen,
- Pornographie zugänglich zu machen und zu erwerben,
- kinderpornographische Schriften abzurufen,
- zu Straftaten anzuleiten oder
- Gewalt zu verherrlichen oder zu verharmlosen,
- alle Formen des Cybermobbings,
- unaufgefordert Nachrichten oder Informationen an Dritte zu Werbezwecken (Spamming) zu versenden

Der Endnutzer/die Endnutzerin hat alle erforderlichen und üblichen Sicherungsmaßnahmen gegen die ungewollte und missbräuchliche Nutzung des WLANs über die von ihm/ihr eingesetzten IT-Systeme durch unbefugte Dritte zu treffen. Soweit der Endnutzer/die Endnutzerin eine ungewollte oder missbräuchliche Nutzung eines Hotspots über ein von ihm/ihr eingesetztes IT-System feststellt, hat er/sie die Schule unverzüglich zu unterrichten.

##### 5. Nutzung der WLAN Hotspots und Nutzung von Informationen aus dem Internet

Der Internet-Zugang soll grundsätzlich nur für Zwecke genutzt werden, die mit der Schulausbildung zusammenhängen. Hierzu zählt auch ein elektronischer Informationsaustausch, der unter Berücksichtigung seines Inhalts und des Adressatenkreises mit dem Unterricht an der Schule im Zusammenhang steht.

- Schüler/innen dürfen nur zu Themen recherchieren, die vorher mit der Lehrkraft abgesprochen wurden.
- Alle Schüler/innen nutzen das Internet in der Schule nur "als Gast". Es ist ihnen untersagt, online einzukaufen und sich auf externen Seiten als Mitglied anzumelden.
- Kostspflichtige Dienste, Bestellungen oder Verträge dürfen nicht über den schulischen Internetzugang abgeschlossen werden!
- Das Benutzen von WeChat, WhatsApp, Facebook, SMS, Instagram, TikTok und derartigen Webdiensten bzw. Seiten ist nicht gestattet.

Jeder Benutzer verpflichtet sich, keine Software (EDV oder andere Anwendungen wie Apps, etc.) herunter zu laden, zu senden bzw. zu empfangen oder anderweitig zu veröffentlichen. Weiterhin verpflichtet sich jeder Benutzer, im Internet keine Inhalte herunter zu laden oder zu veröffentlichen, die folgende Bedingungen erfüllen:

- Daten oder Komponenten mit Viren, Würmern, Trojanischen Pferden oder sonstigen schadensverursachenden Inhalten.
- Werbung, Bekanntmachung oder Angebote für Güter oder Dienste aus kommerziellen oder parteipolitischen Gründen, die von der Lehrkraft nicht genehmigt wurden.

Das Herunterladen von großen Dateien oder Anwendungen ist nur mit Einwilligung der betreffenden Lehrkraft zulässig. Weiterhin untersagt ist:

- die Beeinträchtigung des Netzbetriebes durch ungezielte und übermäßige Verbreitung von Daten bzw. durch unsachgemäßen Einsatz von Hard- und Software
- die unangemessene Beeinträchtigung des Datenverkehrs anderer Nutzer.
- jede Art des Mithörens oder Protokollierens von fremden Datenübertragungen, des unberechtigten Zugriffs auf fremde Datenbestände oder der unberechtigte Zugang zu fremden Rechnern.
- die Verwendung fremder bzw. falscher Namen oder die Manipulation von Informationen im Netz.

Festgestellte Störungen, Passwortverlust oder Missbrauch durch Dritte sind unverzüglich der betreuenden bzw. zuständigen Lehrkraft zu melden.

## 6. Datenschutz und Datensicherheit

Die einschlägigen datenschutzrechtlichen Vorschriften des Telekommunikationsgesetzes (TKG) und der Datenschutzgrundverordnung (DSGVO) sind einzuhalten. Verkehrsdaten werden durch die BBS3 Oldenburg nach den gesetzlichen Vorgaben des TKG erhoben, verarbeitet und gespeichert. Dies umfasst die IP-Adresse und die MAC-Adresse des Endgerätes, die personenbezogene Berechtigungskennung, Nutzungszeit und -dauer, sowie die URL-Einlogdaten. Darüber hinaus behält sich die BBS3 Oldenburg vor, Daten zu statistischen Zwecken auszuwerten. Die Fristen des TKG zum Löschen von Daten werden eingehalten. Strafverfolgungsbehörden werden die Daten entsprechend den Regelungen des TKG übermittelt.

Der Datenschutzbeauftragte der BBS3 Oldenburg ist zu erreichen unter [datenschutz@bbs3-ol.de](mailto:datenschutz@bbs3-ol.de)

## 7. Sonstiges

Die BBS3 Oldenburg behält sich das Recht vor, diese Nutzungsbedingungen in Zukunft zu aktualisieren. Die jeweils gültige Fassung wird in der Schule – z.B. am Schwarzen Brett- und auf der Homepage veröffentlicht.

Zuwiderhandlungen gegen diese Nutzungsordnung können neben dem Entzug der Nutzungsberechtigung schulordnungsrechtliche Maßnahmen zur Folge haben. Bei Verstoß gegen gesetzliche Bestimmungen sind weitere zivil- oder strafrechtliche Folgen nicht auszuschließen.

## Videokonferenzsysteme

---

### Regeln für Webkonferenzen und Fernunterricht

- Bei Webkonferenzen und im Fernunterricht dürfen mittels MS Teams keine Daten nach Art. 9 Datenschutzgrundverordnung (Gesundheitsdaten, personenbezogene Daten aus denen rassistische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder Gewerkschaftszugehörigkeit sowie Daten zum Sexualleben oder der sexuellen Orientierung hervorgehen) verarbeitet werden.
- Es ist grundsätzlich verboten, Gespräche und Übertragungen mitzuschneiden, aufzuzeichnen, zu speichern auch mit jeder Art auch mit Drittsoftware oder bspw. Handycams ..., außer dass die Lehrkraft dies erlaubt.
- Es ist generell untersagt, dass ein Dritter (auch Eltern, Freunde Geschwister usw.) beim Fernunterricht zuhören zusehen oder sonst wie einen Einblick in die Kommunikation erhalten.
- Der persönliche Account für den Zugang zur Webkonferenz bzw. zum Fernunterricht darf an keine andere Person weitergegeben werden.
- Keine Nutzung in öffentlich zugänglichen Räumen wie z.B. Cafés, Kneipen, Restaurants, ÖPNV, Warteräume, Arztpraxen, Läden usw.