Nutzungsbedingungen zur kostenfreien Nutzung des WLAN – Solveigs Ferienwohnung

Wir freuen uns, dass wir Ihnen Internet kostenlos zur Verfügung stellen zu können. Wenn Sie diesen Service nutzen möchten, müssen Sie mit den folgenden Bedingungen einverstanden sein:

1. Das Internet ist kein rechtsfreier Raum. Es gilt Regeln zu beachten, die den Umgang im Internet zu einem Miteinander führen sollen. Nehmen Sie sich Zeit, diese Nutzungsbedingungen zu lesen.
2. Dieses Funk-Netz (WLAN) ist eine freiwillige, kostenfreie Dienstleistung für Gäste von „*Solveigs Ferienwohnung*“. Wir versuchen den WLAN-Dienst so zuverlässig und sicher wie möglich zu betreiben. Trotzdem gilt: Sie installieren und nutzen das WLAN auf eigenes Risiko. Wir übernehmen keine Garantie für Verfügbarkeit und Sicherheit, sowie keine Haftung für eventuelle Schäden.
3. Die Datenübertragung im WLAN ist abhörbar. Der Internet-Verkehr über unser Portal ist - wie bei öffentlichen Hotspots üblich - **nicht** verschlüsselt. Wer Datennetze benutzt oder seinen Rechner auch nur daran anschließt, geht das Risiko ein, dass sein Rechner missbraucht wird und seine Daten ausspioniert, manipuliert oder gelöscht werden. Angriffe aus dem Internet oder im Gästenetz können wir nicht verhindern. Für den Schutz Ihres Systems, u.a. durch Personal Firewall und Virenscanner, müssen Sie selbst sorgen.
4. Wir behalten uns vor, den WLAN-Service jederzeit und ohne vorherige Ankündigung und Angabe von Gründen zu unterbrechen und die Verbindungen ins Internet nach Jugendschutz-Aspekten automatisiert zu filtern.
5. Benutzername und Verbindungsdaten (IP-Adresse, MAC (Rechner) - Adresse, Zeiten) speichern und verarbeiten wir, soweit dies zur Leistungs-, Fehler-, oder Missbrauchsanalyse nötig ist. Wir behalten uns zu jeder Zeit das Recht vor, Benutzerinformationen zu offenbaren, wenn dies von uns als erforderlich erachtet wird um geltenden Gesetzen, Bestimmungen, Rechtsverfahren oder Anfragen seitens der Verfolgungsbehörden zu entsprechen.
6. Benutzername und Passwort dürfen nur von Ihnen und nur für die Dauer Ihrer Anwesenheit genutzt werden. Sie müssen sie geheim halten und dürfen sie nicht weitergeben.
7. Bei der Nutzung des Internetzugangs müssen alle bundesdeutschen Gesetze eingehalten werden. So stimmen Sie zu, den Internetzugang **nicht** zu verwenden, um zum Beispiel
    - entehrende, belästigende, drohende oder andere gewalthaltige Äußerungen in Schrift, Bild oder Ton vorzunehmen, die Rechte und das Empfinden anderer Personen beeinträchtigen können.
    - Material oder Informationen zu veröffentlichen, zu versenden, hoch zu laden oder zu verbreiten, die Gottes lästernde, verletzende, obszöne, oder ungesetzliche Inhalte umfassen.
    - Dateien hoch zu laden, die Software oder andere Materialien (z.B. Filme und Musikstücke) enthalten, die urheberrechtlich geschützt sind oder / und andere Besitz- oder Persönlichkeitsrechte berühren, und Sie nicht die entsprechenden Nutzungsrechte besitzen oder über das notwendige Einverständnis verfügen.
    - Dateien hoch zuladen, die Viren oder andere schädigende Programme enthalten.
    - Preisausschreiben oder Kettenbriefe durchzuführen oder weiterzuleiten.
    - Dateien (z.B. Filme oder Musikstücke) herunter zu laden, die von anderen Benutzern eines Internet-Dienstes veröffentlicht wurden, wenn sie erkennen können oder erkannt haben müssten, dass diese nicht legal verbreitet werden.
    - gegen geltendes Recht in irgendeiner Art zu verstoßen.

<u>So funktioniert es:</u>

Sie erhalten von uns Tagesvoucher in gewünschter Menge (max. Anzahl gebuchte Nächte), mit denen Sie sich über unser Portal einloggen. Sobald der Voucher aktiviert wird, läuft unterbrechungsfrei die auf dem Voucher abgedruckte Zeit. Sie können sich innerhalb dieses Zeitrahmens beliebig oft mit dem Logincode erneut einwählen. Danach verwenden Sie einen neuen Voucher.

Mit den oben genannten Nutzungsbedingungen bin ich einverstanden:

Bad Münstereifel, den_____

_____ _____

Name des Gastes in Blockbuchstaben Unterschrift des Gastes

"Deutschland sicher im Netz e.V." gibt Tipps für die sichere Nutzung von öffentlichen WLAN-Hotspots.

1. Netzwerkeinstellungen überprüfen. Vor der Nutzung des öffentlichen Internetzugangs sollten Surfer unbedingt die Netzwerkeinstellungen des eigenen Betriebssystems überprüfen. Die Funktion "Dateifreigabe" ist zu deaktivieren: Dafür klickt man im Windows-Betriebssystem das Verzeichnis "C:\Dokumente und Einstellungen\Eigene Dateien" mit der rechten Maustaste an und wählt den Menüpunkt "Freigabe und Sicherheit" aus. Andere Hotspot-Nutzer können ansonsten unter Umständen auf die gespeicherten Dateien des eigenen Rechners zugreifen.

2. Hotspot manuell auswählen. Die Anmelde- und Zugangsdaten des Hotspots müssen stimmen. Daher sollten Surfer den Hotspot grundsätzlich manuell auswählen. Eine automatische Verbindungsaufnahme durch das Betriebssystem ist nicht zu empfehlen.

3. Vorsicht bei sensiblen Daten. Für den Umgang mit persönlichen Daten gilt beim Surfen in öffentlichen Hotspots besondere Vorsicht. Benutzernamen und Passwörter sollten unbedingt verdeckt eingegeben werden. Hochsensible Daten wie etwa beim Online-Banking sollten grundsätzlich nicht übertragen werden. Wer dennoch per Hotspot Geld überweisen muss, muss auf die Verschlüsselung der Verbindung achten. In der Adressleiste des Browsers sollte dann "https://" statt http:// vor der eigentlichen Adresse stehen. Zudem ist ein Schloss-Symbol erkennbar.

4. Neuesten Webbrowser nutzen. Moderne Browser prüfen beim Surfen, ob die Zertifikate für sichere Verbindungen noch gültig sind. Daher sollte immer die neueste Version des Webbrowsers verwendet werden.

5. Verbindungsdauer so kurz wie möglich halten. Um Hackern wenig Chancen für einen Angriff zu geben, sollten öffentliche Hotspots möglichst kurz genutzt werden. Stundenlanges Surfen ist bei der drahtlosen Internetnutzung im Hotel oder Café nicht zu empfehlen.

6. Vor Viren und Schadprogrammen schützen. Wie beim Surfen über ein Kabel gilt auch bei der drahtlosen Internetnutzung: Virenscanner, Firewalls und weitere Sicherheitsvorkehrungen müssen aktiviert und auf dem neuesten Stand sein. Zudem sollten Surfer nur mit eingeschränkten Benutzerrechten ins Netz gehen. Das erschwert die Installation von Schadprogrammen durch Dritte. Nach der Online-Sitzung sollten die Drahtlosschnittstellen (WLAN, Bluetooth, Infrarot) wieder deaktiviert werden.