



**ISTITUTO D'ISTRUZIONE SECONDARIA SUPERIORE
"RINALDO D'AQUINO"**

C.F. 91010430642 – Cod. Mecc. AVIS02100B

e-mail avis02100b@istruzione.it **P.E.C.** avis02100b@pec.istruzione.it



hirpina audacia

Liceo Scientifico – Liceo delle scienze umane – Liceo Musicale
Via Scandone – 83048 Montella (AV)
Segreteria: 0827 1949166 fax: 0827 1949162 - Dirigente Scolastico: 0827 1949161
Liceo Classico - Via Fontanelle, 1 - 83051 Nusco (AV) - 0827 64972
Istituto Tecnico - settore Tecnologico - ind. Informatica e Telecomunicazioni art. Informatica
Ind. Chimica, materiali e biotecnologie art. Biotecnologie ambientali
Ind. Elettronica ed elettrotecnica art. Automazione
Via Verteglia – 83048 Montella (AV) 0827 1949183 - fax 0827 1949182
Istituto Tecnico - settore Tecnologico - ind. Meccanica, mecatronica ed energia art. Energia
Via Tuoro – 83043 Bagnoli Irpino (AV) - tel 0827 62268
Unità Didattica II livello rete territoriale CPIA (già corso serale SIRIO)-Istituto Tecnico - settore
Tecnologico - ind. Meccanica, mecatronica ed energia art. Energia
Via Tuoro – 83043 Bagnoli Irpino (AV) - tel 0827 62268



REGOLAMENTO RETE

I.I.S.S. Rinaldo d'Aquino

Art.1 Premessa

Il nostro istituto favorisce lo sviluppo delle nuove tecnologie informatiche e multimediali per integrare i tradizionali processi di insegnamento-apprendimento con l'uso di metodologie innovative e strumenti tecnologici che possano offrire opportunità e modalità diverse, ma altrettanto efficaci, per conseguire specifici obiettivi formativi.

La scuola limita l'accesso ad Internet mediante un filtro per la navigazione, implementato dal firewall di rete, e tutte le attività in rete vengono adeguatamente monitorate e tracciate nel rispetto delle vigenti normative sulla privacy. Il filtro potrebbe non eliminare tutti i rischi perché è possibile commettere eventuali errori o riscontrare tentativi o attività illegali anche su siti leciti.

Per questi motivi i docenti hanno la responsabilità di guidare gli studenti durante le attività online, di stabilire obiettivi ben chiari nell'uso di Internet, evidenziando le opportunità e i rischi connessi all'uso della comunicazione tecnologica, e devono adoperarsi per sensibilizzare ed educare gli studenti all'uso accettabile e responsabile dei nuovi strumenti di comunicazione, secondo le regole di buon comportamento – che vengono identificate con il nome di Netiquette 2.0 – basate sui principi di collaborazione e di condivisione diretta degli utenti di Internet e dei suoi servizi.

Il presente Regolamento per l'uso accettabile e responsabile della Rete della scuola, deliberato dal Consiglio di Istituto e dal Collegio dei Docenti, è pubblicato sul sito ufficiale della scuola www.iissrinaldodaquino.edu.it e viene sottoscritto dai docenti, dagli studenti e dai genitori.

Tutti gli utenti della rete Internet di istituto devono rispettare scrupolosamente questo Regolamento, le leggi vigenti in materia di diritto d'autore e di tutela della privacy, nonché conoscere e rispettare le specifiche norme penali relative al settore informatico e della comunicazione telematica, nel quadro delle disposizioni generali di legge a tutela del rispetto della persona e della collettività.

Articolo n. 2 - Regole generali di utilizzo della rete

Ogni utente abilitato all'uso della rete wired e wireless dell'Istituto è autorizzato ad utilizzare il servizio esclusivamente per i fini istituzionali per cui è stato concesso. E' vietato fornire a soggetti non autorizzati l'accesso alla rete dell'Istituto, collegarvi apparecchiature o servizi o software non autorizzati, compromettere la sicurezza della rete in qualsiasi modo. L'utente è direttamente responsabile delle attività svolte durante la connessione in internet tramite il servizio wi-fi e wired. È vietato cercare di accedere senza

autorizzazione ai dati o violare la riservatezza di altri utenti, compresa l'intercettazione o la diffusione di password e ogni altro "dato personale" come definito dalle leggi sulla protezione della privacy. È vietato svolgere sulla rete ogni altra attività non consentita dalla vigente normativa, nonché dai regolamenti scolastici adottati.

Tutti gli utenti che accedono alla Rete sono riconosciuti e identificati. Le attività potranno essere controllate dal personale autorizzato nel caso di uso illecito della Rete.

Articolo n. 3 - L'accesso alla rete WiFi

L'accesso alla rete WiFi dell'Istituto è consentito ai membri del personale docente attivi, in coerenza con le finalità didattiche e organizzative del lavoro scolastico; coloro che, ammessi a svolgere attività all'interno della scuola, corsisti o formatori, manifestino motivate necessità di utilizzo della rete; i membri del personale ATA che svolgono compiti che richiedano una connessione, limitatamente all'esercizio della funzione assegnata; gli studenti, solo con accessi temporanei, richiesti e controllati da docenti per specifiche attività didattiche.

Gli utenti dell'Istituto possono accedere alla wifi con i propri dispositivi mobili o mediante dispositivi presenti in aula/laboratorio, solo per finalità strettamente connesse alla didattica e all'organizzazione della stessa e in nessun caso è consentito l'accesso per finalità contrastanti con quelle della scuola.

L'accesso alla rete wi-fi comporta la sottoscrizione e il rispetto del regolamento relativo all'accesso e all'utilizzazione della rete informatica e telematica della scuola da parte dell'utente.

art.3.1 - Diritti e credenziali di accesso

L'accesso al servizio avviene attraverso apposita chiave che resta strettamente personale e che potrà essere associata ad un solo dispositivo. La chiave è a scadenza. Potrà essere rinnovata tramite richiesta da parte dell'interessato.

Per consentire a tutti di poter usufruire del servizio, ad ogni utente è consentito l'utilizzo di un solo dispositivo personale, a propria scelta (PC, tablet, smartphone, ecc.). È responsabilità dell'utente la sicurezza della custodia delle proprie credenziali di accesso alla rete wireless della Scuola.

L'ISS "Rinaldo d'Aquino" non si assume alcuna responsabilità in caso di uso improprio delle credenziali di accesso. Qualora l'utente avesse il sospetto che le proprie credenziali siano state compromesse dovrà comunicarlo tempestivamente al Dirigente Scolastico ovvero al Responsabile di rete. Le infrastrutture ed i servizi sono di proprietà dell'ISS

“Rinaldo d’Aquino”. La stessa Istituzione scolastica potrà interrompere, vietare, bloccare l’accesso ed il servizio, anche a singoli utenti, senza preavviso ed in qualsiasi momento.

4. Regole di comportamento

L’utente si impegna a rispettare le regole di comportamento appresso indicate:

- a. Utilizzare unicamente le risorse per cui il servizio è abilitato: è possibile accedere liberamente ad Internet ma non a tutti i servizi (programmi per lo scambio di file, chat, ecc.). La rete dovrà essere utilizzata per scopo didattico e non personale.
- b. Non tentare azioni di scansione della rete o attacchi alla sicurezza: sono espressamente vietati dalle normative di legge. Inoltre è possibile individuare la provenienza.
- c. Non usare in nessun caso la rete della Scuola per scambiare materiale illegale: lo scambio di materiale protetto da copyright (esempio MP3, film in DivX o DVD, software commerciale, libri di testo, ecc.) è espressamente vietato dalla Legge e soggetto a sanzioni penali. In caso di rilevamento di azioni illegali da parte dell’Amministrazione Scolastica si procederà al richiamo formale dell’utente e si metterà a disposizione dell’Autorità giudiziaria la relativa documentazione.
- d. Non configurare manualmente le impostazioni di rete del proprio apparato: l’infrastruttura di accesso assegna automaticamente i parametri necessari all’utilizzo del servizio. La configurazione manuale dei parametri può comportare malfunzionamenti della connessione per se stessi e per altri utenti.
- e. Non utilizzare la rete wireless per effettuare comunicazioni dirette tra utenti: la banda disponibile non è illimitata, tenerla occupata per comunicazioni di lunga durata limita la possibilità degli altri utenti di accedere ai servizi più efficacemente.
- f. L’utente dovrà dotare il proprio dispositivo di adeguate protezioni contro virus o altro genere di intrusioni. La Scuola non si assume alcuna responsabilità in merito ai dati contenuti nei dispositivi degli utenti del servizio. In caso di aggressione da virus informatico od altro tipo di attacco l’utente non potrà in alcun modo rivalersi sulla Scuola. Si invitano pertanto i fruitori a installare sul proprio apparato software antivirus efficienti ed aggiornati ed un personal firewall adeguatamente configurato.
- g. Ogni responsabilità civile e penale è in capo ai singoli utilizzatori della rete.
- h. Non è consentito l’accesso a siti e servizi che prevedano un traffico di dati sulla rete tali da pregiudicare il buon funzionamento della medesima.
- i. Sono assolutamente vietati collegamenti a servizi P2P (torrent, e-mule, file sharing) o lo scaricamento di contenuti multimediali per finalità ludiche. Sono altresì vietati collegamenti a siti di gioco online.
- j. Custodire le proprie credenziali di accesso alla rete wireless della Scuola.

Art. 5- Informazioni Generali rete

Se ritenuto necessario l'Istituto può disporre dei filtri per contenuti ritenuti non pertinenti alle finalità educative o la tracciatura degli accessi alla rete con contestuale acquisizione delle informazioni legate alle connessioni al servizio erogato, ponendo in essere una memorizzazione di questi dati, utilizzati unicamente allo scopo di prevenire abusi nell'uso della rete.

L'Istituto non è assolutamente responsabile di danni e guasti causati dall'utilizzo dei dispositivi mobili durante la connessione alla rete.

L'Istituto non è responsabile in merito ai contenuti visitati con l'accesso alla rete, alle conseguenze penali e civili derivanti da un uso fraudolento della medesima rete. Ogni responsabilità civile e penale è in capo ai singoli utilizzatori della RWI.

Art. 6 - Reati e violazioni della legge

Al di là delle regole di buona educazione ci sono comportamenti, talvolta solo apparentemente innocui, che possono portare gli autori a commettere veri e propri reati e, di conseguenza, a subire procedimenti penali dalle conseguenze molto serie. Si evidenziano alcuni esempi:

Reati informatici

La Legge 547/1993 individua e vieta tutta una serie di comportamenti nell'ambito informatico che sono stati reputati lesivi per gli interessi non solo dei singoli cittadini ma anche di persone giuridiche, in particolare per le imprese e gli enti pubblici:

• Accesso abusivo ad un sistema informatico e telematico

- Attività di introduzione in un sistema, a prescindere dal superamento di chiavi "fisiche" o logiche poste a protezione di quest'ultimo (art. 615 *ter* Codice Penale).
- Per commettere il reato basta il superamento della barriera di protezione del sistema o accedere e controllare via rete un PC a insaputa del legittimo proprietario, oppure forzare la password di un altro utente e più in generale accedere abusivamente alla posta elettronica, ad un server o ad un sito su cui non siamo autorizzati.

- **Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico**

- L'art. 615 *quinquies* del Codice Penale punisce *“chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in lui contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale, l'alterazione del suo funzionamento”*; in altri termini, punisce la produzione e la diffusione dei virus informatici.
- Per commettere questo reato basta, anche solo per scherzo, diffondere un virus attraverso messenger o la posta elettronica, spiegare ad altre persone come si può fare per eliminare le protezioni di un computer, un software o una console per giochi oppure anche solo controllare a distanza o spegnere un computer via rete.

- **Danneggiamento informatico**

– Per danneggiamento informatico si intende un comportamento diretto a cancellare o distruggere o deteriorare sistemi, programmi o dati. L'oggetto del reato, in questo caso, sono i sistemi informatici o telematici, i programmi, i dati o le informazioni altrui (art. 635 Codice Penale).

- **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici**

– Questo particolare reato è disciplinato dall'art. 615 *quater* Codice Penale e si presenta spesso come complementare rispetto al reato di frode informatica.

- Commette questo reato colui che si *“procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo”* (art. 615 *quater* Codice Penale).
- E' considerato reato anche quando l'informazione viene carpita in modo fraudolento con “inganni” verbali e quando si prende conoscenza diretta di documenti cartacei ove tali dati sono stati riportati osservando e memorizzando la “digitazione” di tali codici.

- Si commette questo reato quando si carpiscono, anche solo per scherzo, i codici di accesso alla posta elettronica, al messenger o al profilo di amici e compagni.

• Frode telematica

- Questo reato discende da quello di truffa e viene identificato come soggetto del reato *“chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno”* (art. 640 ter Codice Penale).
- Il profitto può anche *“non avere carattere economico, potendo consistere anche nel soddisfacimento di qualsiasi interesse, sia pure soltanto psicologico o morale”* (art. 640 ter Codice Penale).
- Il reato di frode telematica sovente viene a manifestarsi unitamente ad altri reati informatici, quali l'accesso informatico abusivo e danneggiamento informatico in conseguenza alla detenzione e diffusione abusiva di codici di accesso a sistemi informatici o diffusione di programmi diretti a danneggiare o interrompere un sistema informatico.

Reati non informatici

• Ingiuria

- Chiunque offende l'onore o il decoro di una persona commette il reato di ingiuria.
- Incorre nello stesso reato chi commette il fatto mediante comunicazione telegrafica o telefonica o con scritti o disegni diretti alla persona offesa (art. 594 del Codice Penale).

• Diffamazione

- Qualcuno che offende la reputazione di qualcun altro quando, all'interno di una comunicazione con più persone, si diffondono notizie o commenti volti a denigrare una persona (art. 595 Codice Penale).
- Aggravante nel caso in cui l'offesa sia recata con un "mezzo di pubblicità" come l'inserimento, ad esempio, in un sito web o Social network di una informazione o un giudizio su un soggetto.
- La pubblicazione online dà origine ad un elevatissimo numero di "contatti" di utenti della rete, generando una incontrollabile e inarrestabile diffusione della notizia.

• **Minacce e molestie**

– Il reato di minaccia consiste nell'indirizzare ad una persona scritti o disegni a contenuto intimidatorio per via telematica (art 612 Codice Penale).

- Può capitare che alcune minacce vengano diffuse per via telematica anche per finalità illecite quali, ad esempio obbligare qualcuno a "fare, tollerare, omettere qualche cosa" (violenza privata art. 610 Codice Penale) o per ottenere un ingiusto profitto (estorsione art. 629 Codice Penale).
- Sull'onda di questa tipologia di reati è utile descrivere anche quello di "molestie e disturbo alle persone", disciplinato dall'art. 660 Codice Penale, che si fonda sul contattare da parte di terzi, per finalità pretestuose, il soggetto i cui dati sono stati "diffusi" per via telematica (ad esempio la pubblicazione del nominativo e del cellulare di una persona online, accompagnato da informazioni non veritiere o ingiuriose, potrebbe indurre altre persone a contattare la persona per le ragioni legate alle informazioni su questa fornite).

• **Violazione dei diritti di autore**

- La Legge 159/1993 sottolinea all'art. 1 che chiunque abusivamente riproduce a fini di lucro, con qualsiasi procedimento, la composizione grafica di opere o parti di opere letterarie, drammatiche, scientifiche, didattiche e musicali, che siano protette dalle norme di legge, ovvero pone in commercio, detiene per la vendita o introduce a fini di lucro le copie viola i diritti di autore.

Art. 7 - Operazioni non autorizzate sulla rete della scuola

E' vietato installare programmi non autorizzati su tutte le postazioni informatiche della scuola. Qualora fosse necessario, solo ed esclusivamente per fini didattici e non per scopi personali, installare software non in dotazione alla scuola, l'interessato dovrà produrre apposita richiesta motivata direttamente al Dirigente Scolastico. Solo dopo la relativa autorizzazione si potrà procedere all'installazione del software.

Art. 8 - Sanzioni

A fronte di violazioni del Regolamento, la scuola, su valutazione del Dirigente Scolastico, si assume il diritto di impedire l'accesso dell'utente a Internet per un certo periodo di tempo, rapportato alla gravità del fatto.

La violazione o il dolo accertati, oltre all'intervento disciplinare, daranno luogo alla richiesta di risarcimento delle ore perse per ripristinare il sistema e renderlo nuovamente operante ed affidabile; rimangono comunque applicabili ulteriori sanzioni disciplinari, azioni civili per danni, nonché l'eventuale denuncia del reato all'Autorità Giudiziaria.

Nel caso di infrazione consapevole da parte dei docenti o del personale non docente sarà compito del Dirigente Scolastico intervenire per via amministrativa secondo le norme vigenti.