Regolamento per l’accesso alla rete Wi-Fi

1. Norme generali sull’attività di navigazione

Gli utenti che accedono tramite connessione Wi-Fi dell’Istituto alla rete scolastica e alle risorse da questa accessibili (dispositivi, applicazioni, dati, accesso ad Internet) utilizzando credenziali di accesso messe a disposizione dalla scuola sono tenuti a utilizzare tali risorse in modo corretto e responsabile, in accordo con gli scopi didattici e informativi per i quali è fornita.

2. Registrazione ed accesso al servizio

L’utilizzo dell’accesso è consentito al solo personale autorizzato.
L’utente riceve le proprie credenziali di autenticazione, la cui scadenza dipende dalla *classe di utenza* a cui appartiene (personale docente, personale non docente, a tempo determinato o indeterminato, ospiti esterni, etc.). Le credenziali saranno automaticamente disattivate alla loro scadenza.

3. Finalità e restrizioni

L'accesso alla rete Wi-Fi dell'Istituto (indicata di seguito come la “rete”) è consentito per finalità didattiche, amministrative o di manutenzione della rete; in nessun caso è consentito accedervi per finalità contrastanti con quelle della scuola.
In nessun caso o circostanza gli utenti abilitati sono autorizzati a compiere attività illegali utilizzando le risorse di proprietà dell’Amministrazione.
Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

1. Violazioni dei diritti di proprietà intellettuale di persone o società, o diritti analoghi includendo, ma non limitando, l’installazione o la distribuzione di copie pirata o altri software prodotti che non sono espressamente licenziati per essere usati dall’Amministrazione.
2. Copie non autorizzate di materiale protetto da copyright (diritto d’autore) includendo, ma non limitando, digitalizzazione e distribuzione di foto e immagini di riviste, libri, musica e ogni altro software tutelato per il quale l’Amministrazione o l’utente finale non ha una licenza attiva.
3. È rigorosamente proibita l’esportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali ed internazionali.
4. Il collegamento a servizi P2P (inclusi torrent, e-mule, file sharing) o lo scaricamento di contenuti multimediali per finalità ludiche (es. siti di gioco online) o in contrasto con la normativa vigente in materia di violazione della proprietà intellettuale.
5. Introduzione di programmi maliziosi nella rete o nei sistemi dell’Amministrazione.
6. Rivelazione delle credenziali personali ad altri o permettere ad altri l’uso delle credenziali personali.
7. Usare un sistema dell’Amministrazione (PC o server) per acquisire o trasmettere materiale pedopornografico o che offende la morale o che è ostile alle leggi e regolamenti locali, nazionali o internazionali.

8. Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.
9. Realizzare brecce nelle difese periferiche della rete del sistema informativo dell'Amministrazione o distruzione della rete medesima, dove per brecce della sicurezza si intendono, in modo non esaustivo:
    - accessi illeciti ai dati per i quali non si è ricevuta regolare autorizzazione;
    - attività di "sniffing";
    - disturbo della trasmissione;
    - spoofing dei pacchetti;
    - negazione del servizio;
    - le modifiche delle mappe di instradamento dei pacchetti per scopi illeciti;
    - l'attività di scansione delle porte o del sistema di sicurezza è espressamente proibita salvo deroghe specifiche.
10. Eseguire qualsiasi forma di monitoraggio di rete per intercettare i dati in transito.
11. Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle applicazioni.
12. Interferire o negare l'accesso ai servizi di ogni altro utente abilitato.
13. Usare o scrivere qualunque programma o comando o messaggio che possa interferire o con i servizi dell'Amministrazione o disabilitare sessioni di lavoro avviate da altri utenti di Internet/Intranet/Extranet.
14. Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione.
15. L'accesso a siti e servizi che prevedano un traffico dati sulla rete tale da pregiudicare il buon funzionamento della medesima, laddove non direttamente correlati all'attività didattico-amministrativa.

4. Classi di utenza

Hanno diritto ad accedere alla rete:

a) i membri del personale docente in servizio in questo Istituto, in coerenza con le finalità didattiche e organizzative del lavoro scolastico;
b) utenti esterni: coloro che, ammessi a svolgere attività all'interno della scuola, corsisti o formatori, manifestino motivate necessità di utilizzo della rete;
c) i membri del personale ATA che svolgono compiti che richiedono una connessione, limitatamente all'esercizio della funzione assegnata;
d) il personale tecnico interno o esterno che accede alla rete a scopo di manutenzione.

5. Continuità del servizio

La rete Wi-Fi, nelle zone coperte dal segnale, sarà attiva durante i giorni di apertura della scuola, fatte salve eventuali interruzioni tecniche derivanti da necessità di manutenzione degli apparati o guasti degli stessi o di altra natura non dipendenti dalla volontà dell'Amministrazione.

L'Istituto non garantisce la continuità del servizio o un minimo di banda dati.

6. Filtri e tracciamento accessi al web

L'Istituto si riserva la possibilità di attivare o modificare filtri per contenuti considerati non pertinenti alle finalità didattiche.
Inoltre, è attivo un sistema di tracciamento degli accessi alla rete Wi-Fi, utilizzato unicamente allo scopo di prevenire abusi nell'uso della rete con contestuale acquisizione di informazioni riguardanti le connessioni al servizio erogato (indirizzo IP, indirizzo MAC, host di destinazione). Tale tracciamento è effettuato in conformità alla normativa vigente (Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni).
L'Istituto ha facoltà di modificare criteri e/o strumenti di filtraggio a seconda delle evoluzioni tecnologiche dell'infrastruttura e dell'attività degli utenti.

7. Responsabilità

L'Istituto non è assolutamente responsabile di eventuali danni e guasti causati ai dispositivi degli utenti durante la connessione alla rete.
Allo scopo di garantire l'integrità e la sicurezza del servizio, l'Istituto ha attivato misure di filtro alla navigazione e di tracciamento degli accessi e degli utilizzi della rete Wi-Fi. L'Istituto non è in alcun modo responsabile in merito ai contenuti visitati dai singoli utenti della rete Wi-Fi e alle conseguenze penali e/o civili derivanti da un uso fraudolento della stessa. Ogni responsabilità civile e penale, comprovabile dai log di tracciamento, è in capo ai singoli utilizzatori della rete. L'utilizzatore della rete Wi-Fi è altresì invitato a segnalare tempestivamente agli amministratori della rete stessa ogni attività sospetta e ogni utilizzo non conforme a quanto contenuto nel presente regolamento.

8. Attivazione del servizio

L'abilitazione all'utilizzo della rete Wi-Fi deve essere preceduta, nel rispetto delle normative vigenti, dall'identificazione certa dell'utente, che nel caso di utenti esterni avverrà tramite esibizione di un documento di identità.
Essendo l'attivazione, per motivi di sicurezza, legata a un singolo dispositivo (smartphone, tablet, notebook, ecc.), occorre ripetere la procedura di seguito descritta per ogni dispositivo attraverso il quale l'utente vuole accedere alla rete Wi-Fi.

1. Compilare l'apposito modulo reperibile sul sito web ufficiale dell'Istituto e consegnarlo all'Ufficio Tecnico, che rilascerà le credenziali di accesso (cioè la password della rete e il *voucher personale*).
2. Effettuare il primo accesso alla rete Wi-Fi usando la password ricevuta; a quel punto il sistema di identificazione dirotterà l'utente sul portale di accreditamento dove potrà immettere il voucher personale. **Nota:** il voucher dovrà essere immesso soltanto al primo accesso.

L'autorizzazione all'accesso e alla navigazione su Internet tramite la rete Wi-Fi è comunque subordinata alla dichiarazione di aver preso visione e di accettare le presenti disposizioni.

9. Credenziali di accesso

Le credenziali di accesso (cioè la password della rete Wi-Fi e il voucher personale) saranno consegnati unicamente al richiedente il servizio.

Il sistema identifica l'accesso anche attraverso l'indirizzo MAC del dispositivo utilizzato per la connessione. Pertanto, qualora si volessero usare più dispositivi per connettersi alla rete, occorrerà fare una nuova richiesta di accesso (per ottenere un ulteriore voucher).
Le credenziali di accesso sono personali, non cedibili e utilizzabili esclusivamente dall'utente cui sono state assegnate.
Non è consentito, per nessun motivo, divulgare le proprie credenziali o permetterne l'utilizzo a terzi.
L'utente che ha ottenuto l'accesso alla rete Wi-Fi mediante le credenziali a lui assegnate ha la totale responsabilità delle attività svolte per il tempo di utilizzo del servizio.
L'indebita cessione o utilizzo delle credenziali comporta l'immediata esclusione dal servizio, fatte salve le eventuali maggiori responsabilità che la normativa vigente ponga a carico dell'utente.
L'Istituto si riserva il diritto di disattivare le utenze inutilizzate per periodi continuativi superiori a 30 giorni.

10. Disattivazione del servizio

L'utente può richiedere la disattivazione del voucher personale (ad esempio nel caso di dispositivo non più in uso o di cui non si è più in possesso), compilando l'apposito modulo reperibile sul sito web ufficiale dell'Istituto e consegnandolo all'Ufficio Tecnico.

Appendice: Regolamento Europeo 679/2016 GDPR

Il **Regolamento Generale sulla Protezione dei Dati (GDPR)** stabilisce rigorose norme per la protezione dei dati personali degli utenti, compresi quelli relativi all'accesso alla rete Wi-Fi. Richiamiamo di seguito i criteri fondanti del GDPR, recepiti nel presente Regolamento per l'accesso alla rete Wi-Fi:

Trattamento dei Dati Personali

- **Consenso**: Gli utenti devono essere informati chiaramente e dare il loro consenso esplicito prima che i loro dati personali vengano raccolti e trattati.
- **Minimizzazione dei Dati**: Solo i dati necessari devono essere raccolti e trattati, riducendo al minimo la quantità di informazioni personali memorizzate.
- **Sicurezza dei Dati**: Devono essere adottate misure adeguate per garantire la sicurezza dei dati personali, come la crittografia e la protezione contro accessi non autorizzati.

Diritti degli Utenti

- **Accesso e Trasparenza**: Gli utenti hanno il diritto di accedere ai loro dati personali e di essere informati su come vengono utilizzati.
- **Cancellazione**: Gli utenti possono richiedere la cancellazione dei loro dati personali quando non sono più necessari per il loro scopo iniziale.
- **Portabilità**: Gli utenti hanno il diritto di trasferire i loro dati personali da un fornitore di servizi a un altro.

Responsabilità del Fornitore di Servizi Wi-Fi

- **Valutazione del Rischio**: I fornitori di servizi Wi-Fi devono condurre una valutazione del rischio per identificare e mitigare eventuali rischi per la protezione dei dati.
- **Responsabile del Trattamento dei Dati**: Deve essere nominato un responsabile del trattamento dei dati che garantirà il rispetto delle normative GDPR.
- **Notifica di Violazioni**: In caso di violazione dei dati personali, il fornitore di servizi deve notificare tempestivamente le autorità competenti e gli utenti interessati.

Misure di Sicurezza

- **Autenticazione**: Utilizzo di metodi di autenticazione robusti per verificare l'identità degli utenti.
- **Crittografia**: Protezione dei dati trasmessi tramite crittografia per impedire l'accesso non autorizzato.
- **Filtraggio MAC**: Blocco dell'accesso alla rete Wi-Fi per dispositivi non autorizzati tramite il filtraggio degli indirizzi MAC.

Il GDPR garantisce che i dati personali degli utenti siano trattati in modo sicuro e trasparente, proteggendo la loro privacy e i loro diritti.

Il responsabile della protezione dei dati (R.D.P./D.P.O.) è reperibile ai seguenti contatti:

Dott. Ferdinando Bassi c/o Easyteam.org SRL
Piazza Lorenzo Perosi, 6 – 26886 Sant'Angelo Lodigiano (LO)
email: rpd@easyteam.org.