REGOLAMENTO ACCESSO ALLA RETE TELEMATICA TRAMITE DISPOSITIVI PERSONALI

Premessa

Il presente documento costituisce parte integrante del Regolamento d'Istituto e definisce le regole di accesso tramite dispositivi personali alla rete telematica d'Istituto, nonché le finalità di connessione tramite la medesima.

Art 1. - Principi generali: diritti e responsabilità

L'ITIS "Delpozzo", per finalità esclusivamente connesse alla realizzazione del Piano Triennale dell'Offerta Formativa, dispone di una rete telematica interna con connessione esterna.
Gli utenti che intendono connettere dispositivi personali all'infrastruttura di rete WIFI o WIRED dell'ITIS "Delpozzo" devono effettuarne richiesta assumendosi ogni responsabilità in ordine al suo corretto utilizzo.
Il trattamento dei dati personali derivanti da tale attività avviene in coerenza con le finalità istituzionali e didattiche e conseguentemente ogni attività avviene nel rispetto del Regolamento Europeo 679/2016 (GDPR) e del Codice Protezione Dati (Dlgs. 196/2003 e s.m.i.), dei provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali, nonché in coerenza con la normativa di diritto scolastico applicabile.
L'utilizzo delle risorse informatiche è da intendersi esclusivamente consentito per finalità connesse alle attività scolastiche, amministrative e didattiche/formative.

Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina ed in ogni caso assumendosene la piena ed unica responsabilità.
Previa richiesta scritta al Dirigente potrà essere autorizzata la connessione dei dispositivi individuali alla rete d'Istituto.
Tale autorizzazione ha carattere strettamente personale, in ordine alla quale il richiedente si assume piena ed esclusiva responsabilità di utilizzo.
In ogni caso non sussiste alcun obbligo, da parte dell'Istituzione, di assegnare autorizzazioni di accesso, e queste potranno essere revocate periodicamente dal Dirigente, senza necessità di preavviso e comunque ogni qual volta non ne ravvisi più la necessità.

Art 2. - Norme di carattere generale

1. Il presente regolamento disciplina l'utilizzo delle risorse informatiche, della rete internet e dei dispositivi ammessi, ovvero esclusivamente computer portatile, tablet, e-reader. Nessun altro tipo di dispositivo è ammesso.
2. I dispositivi devono essere usati a scuola esclusivamente per soli scopi didattici e solo dopo previa autorizzazione esplicita del soggetto competente per funzione.
   Ogni utilizzo non autorizzato, al di fuori di quanto previsto in precedenza, non è permesso e sarà sanzionato.
3. Si richiama l'attenzione sulle possibili conseguenze di eventuali riprese audio/video o fotografie effettuate all'interno degli ambienti scolastici, al di fuori dei casi consentiti, e successivamente diffuse con l'intento di violare le norme anche con azioni di cyberbullismo. Tali azioni possono configurare trattamenti illeciti e come tali possibili fonti di risarcimento del danno e, nei casi più gravi, gli estremi di veri e propri reati.
   Previa verifica del rispetto della normativa immagini, audio e video registrati a scuola a fini didattici restano di proprietà della scuola, che potrà utilizzarli internamente e/o pubblicare sui canali di comunicazione per scopi didattici, promozionali.

4. Gli utenti sono responsabili personalmente dei propri dispositivi; è vietato prendere in prestito dispositivi di altri. La scuola non assume in custodia i beni personali e pertanto, in alcun modo, può essere ritenuta responsabile dello smarrimento, furto o danneggiamento dei medesimi che, in nessun caso, dovranno essere lasciati incustoditi.
5. Il dispositivo mobile può essere utilizzato esclusivamente quale strumento funzionale all'apprendimento ed all'insegnamento.
6. La ricarica dello strumento è responsabilità personale e nulla può essere addebitato all'Istituto che, in ogni caso, non garantisce la disponibilità di punti di ricarica.
7. La richiesta di autorizzazione deve essere avanzata utilizzando esclusivamente il modello allegato, che in alcun modo potrà essere alterato nei suoi elementi, pena il rigetto immediato della richiesta.
8. Per quanto attiene gli smartphone vigono le note emanate dal Ministero e dal Regolamento d'Istituto.
9. Il referente per la Rete d'Istituto scolastica si impegna a fornire una connessione internet protetta e controllata da sistemi di monitoraggio del traffico, al fine di garantire una protezione avanzata contro Malware e contenuti pericolosi, in conformità alle disposizioni in materia di protezione dei dati personali (GDPR; Dlgs. 196/2003 come mod. da Dlgs. 101/2018 e s.m.i). e alle norme sulla tutela dei minori. **Tali sistemi non possono essere in alcun modo elusi mediante connessioni personali non autorizzate.**
10. **Ribadendo la puntuale applicazione delle normative vigenti, si ricorda che l'uso del dispositivo personale non è consentito per ricevere/effettuare chiamate, SMS o altro tipo di messaggistica. Non è consentito l'uso di social network (quali ad esempio Instagram, Snapchat, Twitter, Facebook, Whatsapp e altri), videogiochi online e offline o sistemi per la navigazione anonima (VPN). L'uso di Youtube, Vimeo o altri canali video è limitato all'esplicita richiesta di utilizzo da parte del docente.** Il divieto non si applica soltanto all'orario delle lezioni, ma è vigente anche negli intervalli e nelle altre pause dell'attività didattica (ad es. ricreazione, conferenze, laboratori, etc.). L'estensione del divieto d'uso ai momenti di pausa risponde a un'esigenza prettamente educativa, tesa a favorire la socializzazione e le relazioni dirette tra le persone. Qualora sussista una finalità didattica il docente avrà cura di annotare preventivamente sul registro elettronico i software o social del presente comma ammessi durante le lezioni, nonché la finalità didattica.
11. **Il docente è responsabile della vigilanza sugli studenti a Lui/Lei affidati**. Per tale motivo dovrà prestare adeguata attenzione nonché istruire gli studenti ad un uso consapevole e corretto ed intervenire in caso di uso improprio.

Art 3. - Protezione dei Dati Personali ed utilizzo diligente; conservazione dei dati ed informativa

Come raccomandato anche dal Garante per la privacy si richiede un uso diligente del dispositivo a scuola, ricordando che l'utilizzo consentito è soltanto quello relativo all'apprendimento, per uso strettamente personale.
Invece è sempre vietata la diffusione di immagini senza l'autorizzazione del titolare o delle persone ritratte nelle immagini (nel caso di minorenni, in caso di diffusione di immagini occorre il consenso dei genitori/esercenti la responsabilità genitoriale).
Si evidenzia che la diffusione delle immagini al di fuori delle prescritte autorizzazioni è, salvo casi di maggiore gravità (che possono costituire illecito trattamento dei dati personali come da art. 167 Dlgs. 196/2003 e comportare sanzioni penali, oltre al risarcimento del danno in sede civile) priva di liceità e come tale sanzionabile anche disciplinarmente.

I dati informatici ed i log di rete vengono archiviati dall'Istituto in forma crittografata su server interni e mediante servizi conformi al GDPR; l'accesso a tali informazioni, unicamente per ragioni di controllo e verifica, è consentito al solo personale debitamente e previamente a ciò autorizzato.

Si precisa che le misure di sicurezza adottate, come da art. 32 GDPR, vengono revisionate periodicamente e che le eventuali violazioni di sicurezza, ivi comprese le violazioni dei dati (data breaches art. 33 GDPR) vengono gestite secondo la procedura interna prevista dalle disposizioni vigenti, che richiedono il coinvolgimento del Dpo, ai fini di valutare la necessità degli adempimenti successivi (notifica al Garante e comunicazione agli Interessati).

L'Istituto nei confronti degli Utenti, quali Interessati al trattamento, ha fornito Informativa sul trattamento dei Dati Personali, da intendersi richiamata in questa sede; nell'informativa è possibile visionare le finalità e gli scopi del trattamento dati, nonché le modalità di esercizio degli Interessati, come previsti dagli art. 15 e segg. GDPR, da azionarsi mediante mera richiesta all'Istituto.
L'Istituto riserva di fornire ulteriori informative sintetiche in prossimità delle reti, indicando che la rete è per sua natura e per ragioni di sicurezza sottoposta a monitoraggi e controlli tecnici.

Art 4. - Diritti di proprietà intellettuale

1. Gli utenti devono rispettare e proteggere la proprietà intellettuale, pertanto non è ammessa qualsiasi operazione che possa ledere il diritto d'autore o la proprietà intellettuale, ivi comprese, a titolo esemplificativo e non esclusivo, la copia o il plagio di qualsiasi materiale e/o la violazione dei copyright in qualsiasi forma avvenga (es. fare copie illegali di software, musica, giochi o film) e di qualsiasi materiale didattico condiviso prodotto da docenti e da studenti.
2. Si deve attribuire, citare e richiedere il consenso degli autori o creatori delle informazioni o dei media originali.
3. Qualunque prodotto realizzato per le finalità del PTOF attraverso le risorse scolastiche è di proprietà dell'Istituto "Mario Delpozzo".

Art 5. - Doveri degli utenti; comunicazione dati all'Autorità competente

1. Ogni utente deve
- utilizzare la rete e le apparecchiature in modo conforme alla normativa ed alle finalità didattiche di Istituto;
- adottare misure di sicurezza adeguate, ad esempio, garantire di disporre di un sistema antivirus efficiente ed aggiornato per tutta la durata richiesta; applicare password robuste;
- segnalare tempestivamente qualsiasi anomalia o incidente informatico occorso;
- rispettare la riservatezza delle informazioni cui accede e non effettuare accessi ad aree precluse, né consentire l'accesso a terzi.

2. E' espressamente vietato utilizzare account di altri utenti o compiere qualsiasi operazione che possa arrecare danno o pregiudizio, anche potenziale, al sistema informatico di Istituto, agli altri Utenti ed a terzi.
3. Ogni utente è responsabile delle operazioni svolte con il proprio dispositivo, dei siti visitati e delle ricerche effettuate.
4. I dispositivi mobili personali autorizzati alla navigazione dovranno essere accreditati dal responsabile di rete, suo delegato o da tecnico informatico dell'Istituto, che dovrà verificare la presenza di antivirus valido per l'intera durata della richiesta.
   Sarà cura del responsabile della Rete d'Istituto e del personale tecnico definire idonei strumenti atti ad impedire violazioni di norme e comunque idonei a tenere traccia degli utenti connessi al fine di poter comunicare la correlazione utente-atto agli organi di polizia giudiziaria a ciò preposti.
   A tal fine si precisa che i log ed i dati tecnici possono essere comunicati alle Forze dell'Ordine ed all'Autorità nel rispetto delle disposizioni di cui alla Direttiva UE 680/2016 e del Dlgs. 51/2018, nonché nelle modalità e limiti di cui all'art. 2Ter Dlgs. 196/2003.

In caso di emersione di fatti (notizie di reato, anche senza conoscere l'autore) in danno degli Utenti, degli studenti minori o maggiorenni e del personale, il Dirigente, in qualità di pubblico ufficiale, ha l'obbligo di procedere a segnalazione immediata, come previsto dall'art. 331 cpp.

Art 6. - Diritto di ispezione ed obbligo di vigilanza

1. La scuola si riserva di poter disporre verifiche, controlli e monitoraggi sull'uso della rete per motivi di sicurezza informatica e per ragioni disciplinari interne, oltre che per le finalità di emersione dei reati di cui al punto precedente.
   L'Istituto ha dunque facoltà di monitorare gli accessi degli utenti al fine di verificare eventuali abusi ed utilizzi difformi da quanto consentito.
2. La scuola si riserva il diritto di monitorare le attività online degli utenti e segnalare all'autorità preposta eventuali abusi.
   Tale attività non configura comunque un controllo massivo e generalizzato dei contenuti, né tanto meno delle comunicazioni personali degli utenti: ogni attività di verifica e controllo viene condotta nel rispetto della riservatezza, previa informazione ai soggetti coinvolti, a meno che ciò non sia possibile per esigenze di indagini.
3. L'insegnante ha la responsabilità e il dovere di sorvegliare costantemente l'attività informatica degli alunni e di istruire i ragazzi ad un uso "in sicurezza" del dispositivo, monitorando che le indicazioni vengano rispettate. L'insegnante deve segnalare con tempestività al Dirigente Scolastico comportamenti degli alunni in contrasto con il presente Regolamento e al personale preposto eventuali anomalie nella Rete.

Art 7. - Sanzioni per il mancato rispetto del presente Regolamento

1. L'uso della tecnologia, sia essa proprietà della scuola o un dispositivo personale, comporta responsabilità personali. Ci si **aspetta che gli utenti rispettino i Regolamenti adottati dall'Istituto**, **agiscano responsabilmente e rispettino i termini e le condizioni fissate**. **Gli utenti sono incoraggiati a segnalare immediatamente e di persona al Dirigente o ai suoi collaboratori ogni uso improprio o potenzialmente improprio della Rete d'istituto.**
2. Il mancato rispetto delle norme contenute nel presente Regolamento comporterà l'avvio di provvedimenti disciplinari e di sanzioni secondo il Regolamento disciplinare di Istituto e le norme vigenti.
   In particolare, le violazioni al Regolamento ed alle disposizioni possono comportare:
   - sanzioni disciplinari secondo il Regolamento di Istituto e normativa di diritto scolastico vigente;
   - eventuale segnalazione all'Autorità competente per fatti penalmente rilevanti;
   - responsabilità civile per danni arrecati all'Istituto, agli altri Utenti o a terzi.

Regolamento approvato dal consiglio di Istituto nella seduta del 15-10-2025

Allegato tecnico per la gestione, archiviazione e trasmissione dei dati

Titolare del Trattamento: ITIS Delpozzo

Responsabili esterni: gestori dei servizi digitali, aziende e tecnici esterni

Soggetti autorizzati interni: personale docente ed amministrativo/tecnico

Base giuridica: finalità istituzionale/interesse pubblico rilevante in ambito formazione (art. 6 lett. E GPDR)

Dati trattati: log di accesso, indirizzi IP, orari di connessione; utenze

Conservazione: 6 mesi, salvo proroghe motivate

Accesso alle informazioni (log, utenti): solo personale autorizzato; registrazione e verifica periodica degli accessi

Trasmissione all'Autorità: fatti costituenti notizia di reato, anche anonima, come da art. 331 cpp

Comunicazione: PEC istituzionale, richiesta di accesso delle Forze dell'Ordine presso la Sede

Informazioni agli interessati: informativa estesa e sintetica