

REGOLAMENTO UTILIZZO DELLA RETE TELEMATICA E DELLE RISORSE INFORMATICHE

Premessa

Il presente documento costituisce parte integrante del Regolamento d'Istituto e le regole di utilizzo della rete telematica d'Istituto nonché le finalità di connessione tramite la medesima e l'utilizzo dei sistemi informatici di proprietà dell'Istituto

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 avvalersi dell'infrastruttura di rete dell'ITIS "Delpozzo" dovranno effettuare richiesta assumendosi ogni responsabilità in ordine al suo corretto utilizzo

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 assegnate credenziali di accesso univoche ad ogni richiedente. Le credenziali di accesso alla rete sono strettamente personali e vi è espresso divieto di divulgarle a terzi.

In ogni caso **non sussiste alcun obbligo**, da parte dell'Istituzione, di assegnare autorizzazioni di utilizzo 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. - Posto di lavoro

Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione.

Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore. E' pertanto proibito installare qualsiasi programma da parte dell'utente o di altri operatori, esclusi gli addetti autorizzati da Dirigente scolastico.

Ogni utente è personalmente responsabile dei dati memorizzati nel personal computer o in rete tramite il proprio account, nonché di quanto inviato tramite posta elettronica o altri servizi.

Per questo motivo è tenuto ad effettuare il trattamento dei dati secondo le indicazioni emanate dal Titolare del trattamento o suo delegato nonché in ottemperanza alle norme vigenti.

Anche qualora fosse tecnicamente possibile nessun utente potrà prendere visione o copiare dati che eccedano la propria sfera di competenza.

Abusi, attività vietate, attività consentite, obblighi, sanzioni

Si intende con abuso qualsiasi violazione del presente regolamento e comunque di norme civili, penali e amministrative che disciplinano le attività e i servizi informatici svolti sulla rete e di condotta personale.

In particolare è vietato:

1. usare la rete in modo difforme da quanto previsto dal presente regolamento.
1. Usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative.
2. Utilizzare la rete per scopi incompatibili con l'attività istituzionale dell'Itis "Mario Delpozzo".
3. Utilizzare codici di accesso non propri.
4. Cedere a terzi i propri codici di accesso al sistema.

5. Conseguire l'accesso non autorizzato a risorse di rete interne o esterne nonché a datistiche eccedano la propria sfera di competenza
6. Violare la riservatezza di altri utenti o di terzi.
7. Agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti.
8. Agire deliberatamente con attività che distruggano risorse (persone, capacità, elaboratori).
9. Fare o permettere ad altri trasferimenti non autorizzati di informazioni (software, basi dati, ecc.).
10. Installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete; come a titolo esemplificativo virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing.
11. Installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali.
12. Cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi personali.
13. Installare deliberatamente componenti hardware non compatibili con le attività istituzionali.
14. Rimuovere, danneggiare deliberatamente o asportare componenti hardware.
15. Utilizzare le risorse hardware e software e i servizi disponibili per scopi personali.
16. Utilizzare le caselle di posta elettronica per scopi personali e/o non istituzionali.
17. Utilizzare la posta elettronica con la password di altri utilizzatori.
18. Utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi.
19. Utilizzare l'accesso ad Internet per scopi personali.
20. Accedere ad Internet con modalità difformi da quelle consentite.
21. Connettersi ad altre reti senza autorizzazione.
22. Tentare di modificare o raggiungere l'accesso a file, password o dati che appartengano ad altri; monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare files e software di altri utenti, senza averne l'autorizzazione esplicita, fatto salvo, in ogni caso, l'utilizzo dei predetti sistemi da parte del Dirigente o suoi delegati per finalità di monitoraggio del funzionamento della risorse
23. Usare l'anonimato o servirsi di risorse che consentano di restare anonimi.
24. Abbandonare il posto di lavoro senza disconnettere il proprio utente.

Attività consentite

E' consentito all'Amministratore di sistema:

- Monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, per copiare o rimuovere files e software, qualora necessario per attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.
- Creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.
- Rimuovere programmi software non autorizzati, se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.
- Rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

Soggetti che possono avere accesso alla rete

Hanno diritto ad accedere alla rete dell'Itis "Mario Delpozzo" tutti i dipendenti, gli studenti, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, i collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione. L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature.

L'Amministratore di sistema, anche su richiesta del dirigente scolastico, può regolamentare o limitare, o bloccare l'accesso alla rete di determinate categorie di utenti o utenti singoli, quando questo sia richiesto da ragioni tecniche o causa di violazioni alle presenti disposizioni.

Per consentire l'obiettivo di assicurare la sicurezza e il miglior funzionamento delle risorse disponibili l'Amministratore di Sistema può proporre al Titolare del trattamento l'adozione di appositi regolamenti di carattere operativo che gli utenti si impegnano ad osservare.

L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.

Modalità di accesso alla rete e agli applicativi

L'utente che ottiene l'accesso alla rete e agli applicativi è impegnato ad osservare le presenti disposizioni e le altre norme disciplinanti le attività e i servizi che si svolgono via rete ed è impegnato a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi. L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete.

Qualsiasi accesso alla rete e agli applicativi viene associato ad una persona fisica cui imputare le attività svolte utilizzando il codice utente.

Al primo collegamento alla rete e agli applicativi, l'utente deve modificare la password comunicatagli dal Servizio Sistema Informativo e deve rispettare le seguenti norme:

al primo accesso la password ottenuta dal Custode delle password deve essere cambiata.

La password è segreta e non deve essere comunicata ad altri.

La password va custodita con diligenza e riservatezza, in quanto stabilisce un rapporto biunivoco, che permette di responsabilizzare l'incaricato stesso.

La password deve essere costituita da una sequenza non facilmente individuabile.

L'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una rivelazione surrettizia, come in caso di rivelazione volontaria per specifici motivi.

Sanzioni

In caso di abuso o violazione delle norme contenute nel presente regolamento, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dai regolamenti dell'Itis "Mario Delpozzo".

APPROVATO DAL CONSIGLIO DI ISTITUTO IN DATA 21/12/2021