Regolamento interno sull'utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro

Il dirigente scolastico

Visto il Provvedimento del Garante per la Protezione dei Dati Personali 1 marzo 2007 n. 13 (in G.U. n. 58 del 10.03. marzo 2007);

Vista la Direttiva del Dipartimento della Funzione Pubblica 26 maggio 2009, n. 2;

Visto il DPR 16 aprile 2013 n. 62 recante il nuovo Codice di condotta dei dipendenti pubblici;

Visto l'art. 92 del CCNL 2007;

Considerato

- che l'istituzione scolastica, quale datore di lavoro, in persona del dirigente scolastico pro tempore è tenuta ad assicurare la funzionalità ed il corretto impiego degli strumenti ICT da parte dei propri dipendenti, definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa ed adottando le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informativi;

- che a fronte del potere di controllo dell'Amministrazione, datore di lavoro, esiste in capo ai dipendenti l'obbligo, sancito da norme di legge (anche di rilevanza penale) e di contratto, di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa ed idonei a non causare danni o pericoli ai beni mobili ed agli strumenti ad essi affidati, tra i quali vi sono le attrezzature ICT ed i sistemi informativi messi a disposizione dall'Amministrazione;

- che il datore di lavoro (secondo i poteri a lui affidati dalle norme del codice civile, articoli 2086, 2087 e 2104), può riservarsi di controllare l'effettivo adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di lavoro. Nell'esercizio di tali prerogative, tuttavia, deve rispettare la libertà e la dignità dei lavoratori, tenendo presente, al riguardo, quanto disposto dalle norme poste a tutela del lavoratore;

- che l'Amministrazione, tenendo conto delle peculiarità proprie di ciascuna organizzazione ed articolazione di uffici e dei diversi profili professionali autorizzati all'uso della rete, potrà adottare una o più delle misure indicate dalla deliberazione del Garante della privacy 1 marzo 2007 n. 13

Adotta

Il presente regolamento, avente ad oggetto la precisa definizione di criteri e modalità di accesso ed utilizzo ai servizi Internet e posta elettronica da parte del personale dipendente dell'I.P.S.E.O.A. "Caterina de' Medici"

Art. 1 Modalità di utilizzo delle postazioni di lavoro

L'accesso alla rete internet è concessa ai dipendenti quali utenti autenticati e nei limiti stabiliti per ciascun profilo di utenza, così come indicati nelle relative lettere di incarico e nell'informativa loro rilasciata ai sensi dell'art. 13 del D.Lgs. n. 196 del 2003.

Per accedere ai servizi informatici da una postazione di lavoro l'utente deve necessariamente ed obbligatoriamente autenticarsi, utilizzando un codice identificativo (codice utente) e una password.

Verranno a tal fine rilasciati accrediti personali.

Ogni utente è responsabile per il proprio account e per l'uso che ne viene fatto, essendo tenuto a tutelarlo da accessi non autorizzati. Non è ammessa la comunicazione del proprio account a terzi.

L'utente, ha l'obbligo di:

- non cedere, una volta superata la fase di autenticazione, l'uso della propria postazione a persone non autorizzate;

- non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione, provvedendo a bloccare la postazione in caso di allontanamento temporaneo;

- conservare la password nella massima riservatezza e con la massima diligenza;

- spegnere o disconnettersi dal PC al termine del lavoro o in caso di assenze prolungate dalla propria postazione.

- prestare la massima attenzione ai supporti di origine esterna (es. pen drive), verificando preventivamente tramite il programma di antivirus (installato su tutti i PC dei laboratori di informatica) ogni file acquisito attraverso qualsiasi supporto e avvertendo immediatamente l''Amministratore di Sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti.

Art. 2 -– Misure di sicurezza predisposte dall''Istituzione Scolastica

L'utilizzo di Internet è permesso esclusivamente in relazione a finalità istituzionali e connesse all'attività lavorativa.

In ottemperanza al provvedimento del Garante del 01/03/2007, l''Istituzione scolastica ha provveduto ad adottare le seguenti misure organizzative finalizzate alla prevenzione di utilizzi non pertinenti della rete internet:

- individuazione di categorie e liste di siti bloccati (black list) periodicamente aggiornate

  (In Fase di riorganizzazione e aggiornamento sistemi);

- configurazione di sistemi o utilizzo di filtri che prevengano operazioni non correlate all'attività lavorativa etc) (In Fase di riorganizzazione e aggiornamento)

Attualmente le postazioni che accedono a internet a Gardone Riviera sono tutte registrate in maniera univoca tutti i dispositivi adottati (netbook, smartphone, tablet ecc). I laboratori al momento attuale non hanno account personalizzati (per internet è in fase di aggiornamento e riorganizzazione), ma in previsione con account personali tramite implementazioni di Server locali come nell'amministrazione già di fatto, per ora si utilizzano registri cartacei per la registrazione della postazione di lavoro.

I dipendenti dell'amministrazione interna (Uffici) accedono alla postazione di lavoro tramite autenticazione e password, seguono le suddette regole dispongono di un sistema di protezione antivirus con segnalazione automatica all'amministratore di eventuali problematiche.

Per gli utenti che accedono a Internet è vietato:

- reiterare tentativi di accesso a siti bloccati o di cui si è avuta evidenza del fatto che si tratta di siti non appropriati e non consentiti;

- servirsi delle postazioni di accesso a Internet per attività non istituzionali e non connesse ad attività lavorative e per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;

- registrarsi a siti i cui contenuti non siano connessi all'attività lavorativa;

- accedere a siti pornografici, di intrattenimento, ecc.

- utilizzare sistemi di chat non previamente autorizzati e non correlati a finalità istituzionali

Art. 3 Utilizzo della Posta Elettronica

L'utilizzo di posta elettronica è consentito solo per motivi istituzionali e connessi all'attività lavorativa, da parte dei dipendenti ai quali è stata assegnata un'utenza di posta individuale relativa all'ufficio.

L'accesso è consentito in via esclusiva ai dipendenti ai quali sono state comunicate credenziali di autenticazione per l'accesso alla casella di posta.

All'utente di posta elettronica è vietato:

- trasmettere materiale commerciale e/o pubblicitario non richiesto (spamming), nonché permettere che le proprie risorse siano utilizzate da terzi per questa attività;

- prendere visione della posta altrui e simulare l'identità di un altro utente, ovvero utilizzare per l'invio di messaggi credenziali di posta non proprie, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza;

- trasmettere a mezzo posta elettronica dati sensibili, personali o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento della protezione dei dati;

- l'uso della posta elettronica non è comunque consentito per partecipare a forum e/o dibattiti se non per motivi istituzionali, per diffondere notizie non veritiere o quanto altro che abbia contenuto offensivo e discriminatorio, per inviare lettere a catena ovvero messaggi ripetuti.

Art. 4 Controlli previsti e sanzioni

Nel rispetto della normativa vigente richiamata nelle premesse del presente disciplinare, l'istituzione scolastica non procede a verifiche che possano configurare il controllo a distanza dell'attività dei lavoratori.

L'Amministrazione, nella persona del dirigente scolastico, si riserva la facoltà di eseguire controlli in conformità alla legge, sia per eseguire verifiche sulla funzionalità e sicurezza di reti e sistemi, sia per eseguire verifiche sul corretto utilizzo dei servizi Internet e posta elettronica, in conformità a quanto prescritto dal presente disciplinare e, dalla normativa posta a protezione dei dati personali.

I controlli sono posti in essere dal Titolare del trattamento dati coadiuvato dall'amministratore di sistema.

Ci si potrà avvalere di personale esterno, appositamente nominato quale responsabile esterno di trattamento, secondo le previsioni del D. Lgs. 196/2003.

I controlli sono eseguiti tenendo conto del principio di graduazione (par. 6.1 del Provvedimento del Garante per la Protezione dei Dati Personali 1/3/2007) e procederanno come segue:

a) al verificarsi di comportamenti anomali, il dirigente deve effettuare un controllo anonimo su dati aggregati, riferito all'intera struttura amministrativa oppure a sue aree. Il controllo anonimo potrà concludersi con un avviso generalizzato relativo all'utilizzo anomalo degli strumenti dell'amministrazione e con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite ai dipendenti; in assenza di successive anomalie non si effettueranno controlli su base individuale; nel perdurare delle anomalie si procederà a controlli su base individuale o per postazioni di lavoro;

b) in caso di abusi singoli e reiterati si procederà all'invio di avvisi individuali e si eseguiranno controlli nominativi o su singoli dispositivi e/o postazioni di lavoro;

c) in caso di riscontrato e reiterato uso non conforme delle risorse informatiche, verrà attivato il procedimento disciplinare nelle forme e con le modalità di cui al D.lgs. n. 165 del 2001 articoli 55 bis ss. mm. ii. e seguenti.