REGOLAMENTO PER L'UTILIZZO DEL SISTEMA INFORMATICO, DEI TELEFONI " FISSI", DEI "CELLULARI" E DEI " TABLET "

INDICE

Premesse

In via preliminare devesi precisare che il presente Regolamento si applica a:

- tutti i Lavoratori, a qualsiasi titolo inseriti nell'organizzazione scolastica, senza distinzione di ruolo e/o mansione;
- a tutti i collaboratori dell'Amministrazione, a prescindere dal rapporto contrattuale intrattenuto con la stessa

Tanto precisato deve dirsi che l' utilizzo delle risorse informatiche e telematiche del **I.I.S. Piaget-Diaz di Roma** deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro. Pertanto la Istituzione Scolastica ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati. E' evidente, infatti che la progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone la Istituzione Scolastica ai rischi di un coinvolgimento in tema di responsabilità civili ,penali ed amministrative, creando problemi alla sicurezza e all'immagine della Istituzione Scolastica stessa. Per l'Amministrazione l'utilizzo improprio, da parte del Lavoratore, di Posta Elettronica, Internet e telefoni fissi, può pregiudicare il regolare funzionamento delle installazioni tecniche o altri beni o interessi meritevoli di tutela e/o giuridicamente protetti, fra cui:

a) economie dei costi;
b) la capacità di memoria utilizzabile dei server o l'ampiezza di banda disponibile per il collegamento in rete;
c) sicurezza delle applicazioni e dei dati (disponibilità, integrità, confidenzialità);
d) produttività sul lavoro;
e) la reputazione o l'immagine della Istituzione Scolastica;
f) responsabilità oggettiva della Istituzione Scolastica, ex art. 2049 CC, per comportamenti illeciti dei propri dipendenti.

Per il Lavoratore, i rischi derivanti dall'utilizzo di Posta Elettronica, Internet e telefoni , riguardano:

1. la protezione dei dati personali, propri e di terzi, poiché i predetti strumenti lasciano "tracce" del loro uso;
2. la possibilità che l'Istituzione Scolastica, in fase di eventuale legittimo controllo, venga a conoscenza di dati od opinioni personali del Lavoratore;
3. relativamente all'uso di Posta Elettronica e di Internet, l'introduzione di virus, worm, cavalli di Troia o installazioni di programmi estranei nel computer utilizzato dal Lavoratore, con conseguente perdita di tutti o parte dei file salvati sul medesimo computer.

Si ritiene opportuno dettare ,altresì, norme sull'utilizzo della posta elettronica della istituzione scolastica dei telefoni fissi, mobili e tablet.

A tal fine con il presente Regolamento si disciplinano le modalità di utilizzo:

- **del PERSONAL COMPUTER;**
- **della RETE INTERNET E RELATIVA GESTIONE DELLE PASSWORD**
- **dei SUPPORTI MAGNETICI RIUTILIZZABILI (DISCHETTI,CARTUCCE, ECC.....);**
- **dei PC PORTATILI;**

❖ **della POSTA ELETTRONICA DELLA ISTITUZIONE SCOLASTICA dei TELEFONI FISSI,MOBILI E TABLET**

Art.1 Utenti autorizzati all'uso di Internet

Per quanto riguarda l'uso delle dotazioni informatiche e l'accesso ad internet si individuano 4 tipologie di utenti:

- **Personale tecnico**: autorizzato all'uso limitatamente allo svolgimento delle proprie mansioni o alle disposizioni ricevute
- **Personale amministrativo**: autorizzato all'uso per lo svolgimento dell'attività amministrativa
- **Personale docente:** autorizzato all'uso per qualunque attività educativa, didattica e formativa o ad esse anche indirettamente collegata.
- **Alunni**: autorizzati limitatamente all'attività educativa, didattica e formativa programmata dai docenti

Art.2 Utilizzo del Personal Computer

Il Personal Computer affidato al dipendente è uno **strumento di lavoro** per cui ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. La stessa password deve essere attivata per l'accesso alla rete, per lo screen saver e per il collegamento a Internet. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Titolare o del Responsabile interno del trattamento dei dati

Il custode delle parole chiave riservate**,** per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.

Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del Titolare o del Responsabile interno del trattamento dei dati in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente su richiesta del Titolare o del Responsabile interno del trattamento dei dati. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità amministrative, civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 s.m.i. sulla tutela giuridica del software e L. 248/2000 s.m.i. nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita del Titolare o del Responsabile interno del trattamento dei dati.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.

Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …), se non con l'autorizzazione espressa del Titolare o del Responsabile interno del trattamento dei dati.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Responsabile interno del trattamento dei dati nel caso in cui vengano rilevati virus.

Art.3 Utilizzo della Rete

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.

Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

il Responsabile interno del trattamento dei dati può in qualunque momento dare disposizioni di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

L' utente deve effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità necessità la stampa in corso può essere cancellata.

Art.4 Uso della Rete Internet e dei relativi servizi

Il PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa: pertanto è assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal responsabile interno del trattamento dei dati.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal Titolare o dal responsabile interno del trattamento dei dati personali e con il rispetto delle normali procedure di acquisto.

È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

Art.5 Gestione delle Password

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal custode delle password, su disposizione del Responsabile Interno del Trattamento dei dati È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati sensibili e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al Custode delle chiavi.

Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; **;** devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato .

La password deve essere immediatamente sostituita, dandone comunicazione al Custode delle chiavi, nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Responsabile interno del trattamento dei dati.

Art.6 Utilizzo di PC portatili

L'utente è responsabile del PC portatile assegnatogli dal Responsabile del Trattamento dei Dati e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo sul luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni, stage, viaggi d'istruzione , ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

Art.7 Utilizzo dei Supporti Magnetici

Tutti i supporti magnetici riutilizzabili contenenti dati particolari previsti dagli artt. 9 e 10 GDPR 679/2016 devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Terzi particolarmente esperti, infatti, potrebbero recuperare e impossessarsi dei dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici contenenti i prefati dati particolari devono essere custoditi in archivi chiusi a chiave.

Art. 8 Uso dei telefoni "fissi" sul posto di lavoro

1. I telefoni "fissi" che l'Amministrazione mette a disposizione devono essere utilizzati in modo strettamente pertinente allo svolgimento dell'attività lavorativa, secondo un utilizzo appropriato, efficiente, corretto e razionale.
2. Solo in caso di particolare necessità e/o urgenza, i Lavoratori possono utilizzare tali beni per motivi non attinenti l'attività lavorativa e, comunque, non in modo ripetuto o per periodi di tempo prolungati. E' comunque preferibile, laddove possibile, che i Lavoratori utilizzino i propri telefoni cellulari.
   Al fine di consentire il monitoraggio dei costi delle linee telefoniche, verrà fornito al Titolare del trattamento l'elenco delle telefonate effettuate dagli apparecchi di propria competenza completo di numeri telefonici chiamati (con le ultime tre cifre oscurate) e del relativo costo.

3.L'Amministrazione raccoglie i log files per redigere analisi statistiche dirette al perseguimento di finalità organizzative, produttive e di sicurezza.
I dati raccolti, che sono trattati nel rispetto delle leggi di volta in volta in vigore, vengono conservati per il tempo strettamente necessario alle suddette analisi e finalità. In caso di anomalie riscontrate nelle modalità di utilizzo del telefono aziendale, si applicherà quanto previsto dall' art. 13 del presente disciplinare.

Art. 9 Uso dei telefoni "cellulari" e dei "palmari"

1.I telefoni "cellulari" e " tablet " che l'Amministrazione può mettere a disposizione, su richiesta motivata del Dipendente,devono essere utilizzati in modo strettamente pertinente allo svolgimento dell'attività lavorativa, secondo un utilizzo appropriato, efficiente, corretto e razionale.
2. Il Lavoratore assegnatario di un telefono "cellulare", di un " tablet dell'Amministrazione è responsabile del suo utilizzo e della sua custodia.
3. All'utilizzo del telefono "cellulare", o del "palmare" dell'Amministrazione si applicano le medesime regole previste

Art.10 Intranet e dominio istruzione.it

I servizi di posta elettronica del dominio ***istruzione.it,*** quelli forniti dal sito ***www.istruzione.it*** e dalla intranet ministeriale sono direttamente gestiti dalla **Direzione Generale per i Sistemi Informativi** che ha diffuso specifiche informative in merito alle modalità di utilizzo dei suddetti servizi.

Art. 11 Utilizzo del servizio di Posta Elettronica della Istituzione Scolastica

- La Posta Elettronica che l'Istituzione Scolastica mette a disposizione deve essere utilizzata in modo pertinente allo svolgimento dell'attività lavorativa, secondo un utilizzo appropriato, efficiente, corretto e razionale nel rispetto del principio di riservatezza. I Lavoratori assegnatari delle caselle di Posta Elettronica sono responsabili del corretto utilizzo delle stesse e vi accedono mediante autenticazione informatica user-id e password oppure altro sistema identificativo ad es. smart card.
- I Lavoratori sono tenuti, in un'ottica di correttezza ed uso responsabile degli strumenti, a contribuire alla riduzione del fenomeno dello "spam" (trasmissione su larga scala e in grandi volumi di e-mail non sollecitati): evitando di rispondere e/o inviare ad altri destinatari eventuali messaggi, del tipo "catene di Sant'Antonio", non sollecitati, che siano stati ricevuti, ed evitando di comunicare ad altri destinatari, in modo indiscriminato, il proprio indirizzo di posta elettronica o quello di colleghi.
- I Lavoratori non devono condurre attività commerciali di qualsiasi tipo a beneficio proprio e/o di terzi servendosi della Posta Elettronica dell'Istituzione Scolastica .
- E' fatto divieto, in ogni caso, di trasmettere a chiunque a mezzo Posta Elettronica Materiale pornografico, materiale fraudolento/illegale, gioco d'azzardo, materiale blasfemo o molesto/osceno.
  Il predetto divieto riguarda tanto il contenuto quanto gli allegati dei messaggi di Posta.
- I Lavoratori per adempiere il proprio dovere di diligenza e vigilanza nell'utilizzo dei beni e strumenti ad esso affidati hanno l'obbligo di impedire ad altri indebiti utilizzi della propria apparecchiatura informatica, non rilevando, al fine del difetto di responsabilità, il fatto che altri, in sua assenza, abbia potuto usare la postazione lavorativa. In difetto, il comportamento si configura come negligente, inescusabile e gravemente colposo.

Per evitare ogni interferenza con la sfera privata del personale docente e ATA, qualunque comunicazione di interesse amministrativo o di lavoro dovrà avvenire per mezzo delle caselle istituzionali.
La consultazione della posta elettronica da parte dei dipendenti può quindi riguardare:

- caselle personali: su dominio ***istruzione.it***, messa a disposizione da parte del MIUR (e/o casella personale privata, su altro dominio)
- caselle istituzionali di lavoro comunicato dal Responsabile del Interno del Trattamento dei Dasti

A. Uso delle Caselle Personali

Il personale può consultare in orario di servizio caselle personali per motivi legati alla propria attività lavorativa. La gestione deve essere effettuata tramite servizi di "webmail": non è consentito configurare su computer dell'Istituto appositi programmi tipo Outlook o Thunderbird per gestire le proprie caselle personali (anche per garantire al dipendente la dovuta riservatezza).
Nell'uso di caselle personali all'interno della scuola, al dipendente non è comunque consentito:

- inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione della Scuola o del MIUR;
- l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali;
- utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione extra lavorative o azioni equivalenti.

B. Uso delle Caselle Istituzionali Di Lavoro

Le caselle istituzionali sono gestite dagli incaricati del trattamento dei Dati in base ai compiti loro assegnati. In caso di assenza dell'incaricato abituale, questo potrà essere sostituito da altro personale, in base all'organizzazione interna del lavoro disposta da D.S. o D.S.G.A.: quindi tali caselle devono essere utilizzate solo a scopo lavorativo e **NON d**evono essere utilizzate come caselle personali.
Oltre alle disposizioni impartite per l'utilizzo delle caselle personali, si aggiungono le seguenti disposizioni:

- Evitare di aprire messaggi provenienti da mittenti sconosciuti e che contengono allegati sospetti (file con estensione .exe, .scr, .pif, .bat, .cmd,....). In caso di dubbio consultare un tecnico.
- Nel caso in cui si debba inviare un documento all'esterno dell'Istituto, se non specificamente destinato alla modifica, è preferibile utilizzare il formato *.pdf.
- Evitare che la diffusione incontrollata di "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata) limiti l'efficienza del sistema di posta.
- Evitare di inviare allegati di dimensioni eccessive (se necessario usare formati compressi come *.zip, *.rar,...)
- L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali, prima di iscriversi occorre verificare in anticipo se il sito è affidabile.
- La casella di posta deve essere mantenuta in ordine.

Art. 12 I Controlli

1. Qualsiasi forma di controllo venga effettuata, deve essere strettamente necessaria per il Titolare del Trattamento, in relazione a scopi determinati e per il perseguimento di finalità organizzative, produttive e di sicurezza ha facoltà di effettuare qualsiasi forma di controllo necessaria;
2. Nell'eventualità di anomalie riscontrate nell'utilizzo da parte dei Lavoratori degli strumenti di lavoro messi a disposizione dalla Istituzione Scolastica, il Titolare del Trattamento, unitamente al DPO, effettua una prima segnalazione, nella quale non può essere indicato alcun nominativo di Lavoratori, indicando al Responsabile interno o esterno del trattamento il computer nel quale è stata rilevata l'anomalia. Quest'ultimo provvede, a sua volta, ad inviare un avviso generalizzato diretto a tutti i Lavoratori appartenenti alla sua Struttura, nel quale evidenzia l'utilizzo irregolare degli strumenti messi a disposizione dalla Istituzione Scolastica, invitando i Lavoratori ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.
3. Se l'avviso generalizzato di cui al punto 2 non produce effetto e l'anomalia rilevata persiste, il Titolare del trattamento, il DPO e l'Amministratore di Sistema, procedono ad un controllo su base individuale e nominativa, a seguito del quale il Titolare effettua una seconda segnalazione al Responsabile interno indicando l'area presso la quale è inserito il Lavoratore interessato dalle verifiche.
4. Il Titolare del Trattamento nelle funzioni di Dirigente Scolastico, effettuate le necessarie verifiche, attiverà direttamente il procedimento disciplinare nei confronti del Lavoratore ai sensi qualora il fatto sia di gravità tale da comportare una sanzione tra quelle di sua competenza.
   L'Amministrazione è tenuta alla riservatezza in tutte le fasi di accertamento dei fatti;
5. La rilevazione delle anomalie e delle verifiche tecniche di cui ai precedenti punti 2 e 3, è a cura dell'Amministratore di Sistema. Responsabile dei successivi e consequenziali provvedimenti è il Dirigente Scolastico.
6. L'Istituzione Scolastica, nel rispetto del principio di protezione dei dati personali e del divieto di controllo a distanza del Lavoratore, procede, in caso di anomalie, alla conservazione delle "registrazioni a giornale" (log file) relative all'utilizzazione di Internet , della Posta Elettronica e del telefono fisso nonché dei files con il dettaglio dei numeri chiamati totalmente "in chiaro" delle telefonate per il tempo strettamente necessario alla soluzione delle suddette anomalie.

Art. 13: Obbligatorietà e Sanzioni

1. È fatto obbligo a tutti i Lavoratori di osservare le disposizioni portate a conoscenza con il presente Regolamento. La omessa osservanza o la violazione delle regole contenute nel Regolamento è perseguibile con tutte le azioni civili (eventuale risarcimento del danno cagionato).
2. e penali previste dalla legge, nonché con i provvedimenti disciplinari, in conformità a quanto previsto dalle disposizioni normative e contrattuali vigenti per il personale scolastico Il codice di comportamento ed il codice disciplinare sono consultabili nel sito internet della Istituzione Scolastica.

Art. 14 Gestione della casella di Posta Elettronica di un Lavoratore cessato dal servizio

1. In caso di cessazione del rapporto di lavoro l'account di Posta Elettronica del Lavoratore è prontamente bloccato e la sua casella di Posta Elettronica non è più funzionante.
2. I mittenti di email inviate all'indirizzo e-mail bloccato vengono automaticamente informati che l'indirizzo del destinatario è estinto al momento della cancellazione dell'account.

Art. 15: Esercizio dei diritti

I Lavoratori hanno ricevuto informativa sulle modalità di esercizio dei diritti quali previsti dal DGPR 679/2016 in assonanza col D.Lvo 101/2018**.** Comunque:

1. I dati personali inerenti i Lavoratori non possono essere portati a conoscenza di terzi non autorizzati.
2. L'Istituzione Scolastica nell'ambito di procedimenti disciplinari e/o di procedimenti penali di cui all'art. 12 del presente Regolamento e nel rispetto del principio di protezione dei dati personali e del divieto di controllo a distanza del Lavoratore, procede alla conservazione delle "registrazioni a giornale" (log file) relative all'utilizzazione di Internet e/o della Posta Elettronica e/o dei files delle telefonate fino alla conclusione dei relativi procedimenti.
3. Il presente documento viene portato a conoscenza di tutti i Lavoratori mediante pubblicazione nei sito internet.

Art. 16 Aggiornamento e Revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dal Titolare del Trattamento e dal DPO.
Il presente Regolamento è soggetto a revisione con frequenza annuale.

In Roma così dato il 7 gennaio 2019

IL TITOLARE DEL TRATTAMENTO
Dirigente Scolastico
Prof. Scancarello Giovanni
(Firma sostituita a mezzo stampa ai sensi dell'art. 3 co. 2 della L. n. 39/1993)