REGOLAMENTO INTERNO PER LA PROTEZIONE DEI DATI PERSONALI

INDICE

Premessa

Il presente Regolamento Interno, realizzato dalla Casa di Torino dell'Istituto delle Suore di Sant'Anna della Provvidenza (di seguito "Istituto"), ha l'obiettivo di fornire delle linee guida, procedure operative e di buon senso, al fine di eseguire il trattamento dei dati personali, secondo i dettami del GDPR e del codice Privacy, attraverso l'utilizzo degli strumenti organizzativi, informatici e cartacei.
L'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza, liceità e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro; per tale ragione l'Istituto ha adottato il presente regolamento, al fine di fornire delle linee guida per il personale (Garante per la protezione dei dati personali - delibera n. 13 del 1-3-07 pubblicato su G.U. n. 58 del 10/3/07 - "Linee guida del Garante per la posta elettronica ed internet" il quale ha fornito le principali indicazioni per consentire al Datore di Lavoro di adottare internamente le misure a tutela della Sicurezza dei dati trattati e del patrimonio e quella della privacy dei dipendenti).
A fronte di quanto fino ad ora indicato, l'Istituto procederà ad indicare le seguenti regole cui tutti i dipendenti interessati dovranno attenersi, per contribuire alla massima diffusione della cultura della sicurezza ed evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati, oltre che comportamenti illeciti come l'utilizzo di immagini e/o programmi non licenziati e coperti da copyright (Legge n. 633/41).

1. Disciplina concernente l'utilizzo del Personal Computer (hardware e software)

Il Personal Computer affidato al dipendente/collaboratore/stagista è uno **strumento di lavoro**. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione.
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'addetto con la massima diligenza e non divulgata. La password è funzionale per l'accesso alla rete locale.

Non è consentito installare autonomamente programmi provenienti dall'esterno, salvo previa autorizzazione esplicita del Responsabile Informatico o del Titolare del Trattamento, in quanto sussiste il grave pericolo che Virus informatici si inseriscano nel sistema informatico e che quindi alterino la stabilità delle applicazioni dell'elaboratore.
Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal Responsabile del sistema informatico dell'Istituto. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Istituto a gravi

responsabilità civili e penali anche in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. n. 518/92 sulla tutela giuridica del software e L. n. 248/00 sulle nuove norme di tutela del diritto d'autore e succ.mod.) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.
Non è consentito, se non previa autorizzazione del Responsabile Informatico o del Titolare del Trattamento dei dati:

a) modificare le impostazioni di sistema del proprio PC;
b) l'attivazione della password d'accensione (bios);
c) utilizzare proxy esterni e sistemi per la non rintracciabilità del proprio computer,
d) apportare modifiche, delle caratteristiche hardware e software, impostate sul proprio P.C.

Il Personal Computer deve essere spento ogni sera prima di lasciare la rispettiva stanza di lavoro od in caso di assenze prolungate da essa. 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. E' fatto obbligo agli addetti di disconnettere la propria utenza o bloccare il computer ogni volta si lascia la postazione. Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, pen drive, ed altro), se non con l'autorizzazione espressa del Responsabile informatico o del Titolare. Ogni addetto deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Responsabile Informatico o il Titolare del trattamento nel caso in cui vengano rilevati virus.
Le informazioni archiviate digitalmente devono essere esclusivamente quelle previste dalla legge o necessarie all'attività lavorativa.
Non è consentita l'installazione di programmi diversi da quelli autorizzati dal Sistema Informativo Istituzionale, né la riproduzione o la duplicazione di programmi informatici ai sensi della Legge n. 128 del 21/05/2004.
E' vietato diffondere all'esterno dell'Istituto programmi (originali o copie), manuali, documentazione o parti di essa.
È fatto divieto all'Utente scaricare software gratuiti (freeware e shareware prelevati da siti Internet), se non espressamente autorizzato dal Responsabile Informatico o dal Titolare

2. Disciplina concernente l'utilizzo della rete dell'Istituto.

La rete è composta da aree il cui accesso è soggetto a specifiche autorizzazioni e ad unità 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 quest'ultime, vengono svolte regolari attività di controllo, amministrazione e backup.
L'accesso alla rete aziendale è protetto da password; per l'accesso deve essere utilizzato il proprio profilo personale (username e password).
È assolutamente proibito entrare nella rete e nei programmi con altri nomi Utente.
E' fatto divieto di utilizzare la rete aziendale per fini non espressamente autorizzati.

3. Gestione delle Password del S.O. (Sistema Operativo) e della Mail.

Le password di ingresso al S.O. e dello screen saver, sono previste ed attribuite dal Responsabile informatico o dal Titolare.
Le password possono essere formate da lettere e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema (key-sensitive); devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'addetto.
In caso di assenza del dipendente, il Titolare del Trattamento consentirà l'accesso allo strumento elettronico dello stesso, se necessario per poter proseguire l'attività lavorativa. In questo caso il Titolare dovrà fornire comunicazione scritta dell'accesso, alla mail personale del dipendente non presente in casi di estrema urgenza e/o assenza prolungata.

Le password d'ingresso alla rete, di accesso ai vari programmi in rete per i trattamenti dei dati e ad Internet, sono attribuite dall'Istituto. L'addetto è tenuto a conservare nella massima segretezza, la parola di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione.
La password deve essere immediatamente sostituita comunicandolo tempestivamente al Responsabile Informatico o al Titolare, nel caso si ipotizzi/sospetti che la stessa abbia perso la sua segretezza.

4. Disciplina concernente l'utilizzo dei P.C. portatili e supporti magnetici.

L'Utente è responsabile del P.C. portatile assegnatogli dall'Istituto e deve custodirlo con diligenza, sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro; ai portatili si applicano le regole di utilizzo previste per i P.C. connessi in rete con particolare attenzione alla rimozione di eventuali files elaborati sullo stesso prima della riconsegna.
I P.C. portatili utilizzati all'esterno (convegni, visite in azienda, ed altro), in caso di allontanamento, devono essere custoditi in un luogo protetto, inoltre non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i files strettamente necessari.
Nel caso di accesso alla rete aziendale tramite RAS (Remote Access Server)/ VPN (Virtual Private Network): si dovrà utilizzare l'accesso in forma esclusivamente personale, con password; inoltre è obbligatorio disconnettersi dal sistema RAS/VPN al termine della sessione di lavoro.
Tutti i supporti magnetici riutilizzabili (cd-rom, dvd, pen drive USB, hard disk esterni, ecc.) contenenti dati particolari e giudiziari, devono essere trattati con particolare cautela, onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
I supporti magnetici contenenti dati particolari e giudiziari devono essere custoditi in archivi chiusi a chiave.

5. Disciplina concernente l'utilizzo della posta elettronica aziendale.

La Mail assegnata al dipendente, collaboratore e/o stagista è uno strumento di lavoro, in quanto, essa è uno degli **strumenti principali forniti per svolgere l'attività lavorativa.**
La mail del dipendente/collaboratore/stagista, sebbene riporti il nome e cognome (o solo uno dei due) del medesimo, **è di proprietà istituzionale** (mail@). Infatti, in molti casi i contatti con i vari soggetti avvengono solo tramite mail. E' quindi indispensabile, da parte dello Staff coinvolto nel processo di lavorazione, accedere ad ogni comunicazione e quindi accedere a tutte le mail (inviate e ricevute).
Una volta cessato il rapporto di lavoro, sia per dimissioni, licenziamento o termine dello stesso, è necessario disattivare la mail istituzionale associata al dipendente, entro e non oltre 48 ore successive, ed inserire un messaggio per l'Utente finale, indicando l'indirizzo mail a cui rivolgersi.
Tale attività dovrà essere svolta sia per la sicurezza dell'Istituto sia del personale dipendente.
Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
L'account istituzionale deve essere utilizzato solo per fini lavorativi. È vietato l'utilizzo delle caselle di posta elettronica istituzionale ***nomepersona@*** per l'invio di messaggi personali o comunque estranei all'attività lavorativa o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione. È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi.
La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. Si ricorda che tutte gli abbonamenti on-line che impegnano l'Istituto contrattualmente dovranno essere preventivamente autorizzati dalla Direzione.
È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, PEC ed altro).
Si autorizza espressamente la Direzione a visionare la posta elettronica o qualsiasi programma od altro (quindi anche le chat usate impropriamente) in qualunque momento per motivi di sicurezza, oltre che per motivi lavorativi anche in caso di assenza del dipendente.
È obbligatorio controllare gli allegati di posta elettronica prima del loro utilizzo anche se apparentemente innocui o provenienti da fonti attendibili (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

È vietato inviare catene telematiche (o di Sant'Antonio). Non si devono in alcun caso aprire gli allegati di tali messaggi. Nel caso di messaggi provenienti da mittenti conosciuti, ma che contengono allegati sospetti (file con estensione .exe, .scr, pif., .bat .cmd), questi ultimi non devono essere aperti. Utilizzare, nel caso di invio di allegati pesanti, i formati compressi (*.zip *.rar *.jpg). Nel caso in cui si debba inviare un documento all'esterno dell'Istituto è preferibile utilizzare un formato protetto da scrittura (ad esempio il formato Acrobat *.pdf).

6. Disciplina concernente l'utilizzo della rete Internet e dei relativi servizi.

Il PC abilitato alla navigazione in Internet costituisce **uno strumento aziendale** necessario allo svolgimento della propria attività lavorativa.
Poiché l'Istituto deve tutelare il proprio patrimonio di conoscenze da eventuali attacchi informatici, deve ridurre al minimo gli sprechi economici e deve salvaguardare i dati dei terzi riducendo al minimo i rischi derivanti dal trattamento dei dati, l'uso di Internet è concesso solo per le finalità aziendali e pertanto in via preventiva:

- è fatto divieto di navigare su siti non attinenti alle mansioni affidate;
- è fatto divieto di navigare su siti pornografici e siti pedo-pornografici;
- è fatto divieto di navigare su siti che possono rilevare opinioni politiche, religiose o sindacali del dipendente;
- è fatto divieto di effettuare transazioni finanziarie personali (trading online) e acquisti on-line personali;
- è fatto divieto di scaricare o condividere (peer-to-peer) musica, filmati o software;
- è fatto divieto di partecipare a forum per motivi non professionali;
- è fatto divieto di registrarsi a siti i cui contenuti non siano collegati all'attività lavorativa;

Per esigenza di sicurezza aziendale alcune di queste informazioni sono memorizzate temporaneamente (ad esempio, le componenti di file di log eventualmente registrati) ed il Responsabile Informatico vi può accedere legittimamente.

In tutti i casi in cui dalle predette verifiche dovesse risultare il compimento di attività qualificabile come reati, l'Istituto provvederà ad effettuare la comunicazione della notizia di reato alle Autorità Competenti.
È fatto divieto all'Utente scaricare software gratuiti (freeware e shareware prelevati da siti Internet), se non espressamente autorizzato dal Responsabile Informatico o dal Titolare.

7. Protezione antivirus.

Ogni Utente deve tenere comportamenti tali, da ridurre il rischio di attacco al sistema informatico istituzionale mediante virus o mediante ogni altro software aggressivo (ad esempio non aprire mail o relativi allegati sospetti, non navigare su siti non professionali ecc).
Ogni dispositivo magnetico, di provenienza esterna all'Istituto, dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso sia rilevato un virus non eliminabile dal software, non dovrà essere utilizzato.

8. Redazione documenti come PEI, PAI, ecc.

Si fa divieto dell'utilizzo dei dati particolari (relativi allo stato di salute od altro) degli alunni al di fuori dell'istituto scolastico. Per tale ragione, nel momento in cui vengono acquisiti dei documenti, gli stessi devono essere riposti negli appositi armadi protetti.

9. Acquisizione documentazione Sanitaria degli Alunni

Tutta la documentazione relativa al trattamento dei dati sanitari (prescrizioni, assunzioni farmaci salvavita ed altro) non dovrà essere ritirata dai docenti, ma dovrà essere obbligatoriamente consegnata alle Coordinatrici Didattiche. Di tal ché i docenti sono invitati a far presente ai genitori della suddetta procedura.

10. Distruzione dei documenti

Ogni utente nel momento in cui deve eliminare dei documenti contenenti dati personali deve provvedere a distruggerli per il tramite del Distruggi-documenti.

11. Utilizzo dei dispositivi mobili

Si fa divieto di inviare foto e/o materiale contenente dati personali tramite l'uso di dispositivi mobili senza previa autorizzazione.

12. Obbligo di fedeltà.

E' una condizione necessaria che scaturisce dalla stipulazione del contratto di lavoro (L. n.300/70 e CCLN di settore oltre che dalle disposizioni del codice civile) e che sorge in capo al lavoratore subordinato, il quale deve prendersi cura degli interessi dell'Istituto. Il lavoratore e/o collaboratore deve astenersi da atteggiamenti che possano pregiudicare gli interessi dell'Istituto. In particolare il divieto principale riguarda la concorrenza ai danni del datore di lavoro (sia sleale, vietata a chiunque in qualsiasi forma, sia leale).
E' vietato, infatti, diffondere all'esterno dell'Istituto informazioni e documenti, manuali e quant'altro a disposizione dei dipendenti e/o collaboratori.

13. Non osservanza della normativa aziendale.

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento, costituendo inadempimento contrattuale di natura disciplinare o nel caso di violazione delle leggi italiane (artt. 594 - 595 - 600 ter e segg. - 615 bis - 615 ter - 615 quater - 615 quinques - 616 - 617 quater - 617 quinquies - 617 sexies - 618 - 621 -622- 623 - 635 bis - 640 e 640 ter c.p. ed altro), sarà contestato e sanzionato secondo le procedure di cui all'art. 7 della L. n. 300/70, nonché del CCNL applicato dall'Istituto

14. Aggiornamento e revisione.

Il presente Regolamento è soggetto a revisione con frequenza annuale ed entrerà in vigore dalla data di esposizione e Vi sarà consegnato personalmente.

Il presente Regolamento è composto da 4 pagine e tutte le clausole presenti nel suddetto Regolamento, ai punti 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 e 14 sono state lette, confermate e sottoscritte.

Dipendente/collaboratore/stagista

_____

Legale rappresentante

Giulia Grotta

CASA DI TORINO DELL'ISTITUTO
delle Suore di S. Anna della Provvidenza
Via Massena, 36 - 10128 TORINO
Codice Fiscale: 01762810016