Regolamento Privacy per l'utilizzo dei sistemi informatici

dell'Istituto

prot. _____ del _____

Premessa

Premesso che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi ai principi della diligenza e correttezza, normalmente rispettati nell'ambito dei rapporti di lavoro, L'Istituto Scolastico adotta un Regolamento interno finalizzato ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti i soggetti autorizzati, in attuazione del REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Considerato che, inoltre, l'Istituto Scolastico, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, mette a disposizione dei propri dipendenti, a seconda del tipo di funzioni svolte, mezzi di comunicazione efficienti (computer etc.), sono state inserite nel regolamento alcune clausole relative alle modalità ed i doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

La finalità è quella di verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet, muovendo dalla considerazione che prevenire gli abusi debba considerarsi più importante che individuarli.

I principi costituenti il fondamento del presente Regolamento sono gli stessi espressi nel REGOLAMENTO (UE) 2016/679 e nel documento "*Lavoro: le linee guida del Garante per posta elettronica e internet*" del 01/03/2007, e, precisamente:
a) **il principio di necessità**, per il quale l'utilizzo dei dati personali, attraverso l'impiego di sistemi informativi e di programmi informatici, deve essere ridotto al minimo tenuto conto delle finalità perseguite;
b) **il principio di correttezza**, per il quale le caratteristiche essenziali dei trattamenti, siano essi svolti in modalità cartacea o informatica oppure mista (cartacea ed informatica), devono essere partecipate ai lavoratori;
c) **le finalità** alla base del trattamento dei dati personali devono essere determinate, esplicite e legittime, oltre che pertinenti e non eccedenti.

Alla luce dell'art. 4, comma 1, L.n. 300/1970, la regolamentazione della materia indicata nell'art. 1 del presente Regolamento, non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo per consentire a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.

Regolamento

1. Entrata in vigore del regolamento e diffusione

1.1 Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

1.2 Copia del regolamento è a disposizione di ciascun dipendente.

2. Campo di applicazione del regolamento

2.1 Il nuovo regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'Istituzione Scolastica a prescindere dal rapporto contrattuale con la stessa intrattenuto.

2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione.

3. Utilizzo del Personal Computer

3.1 Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente l'attività lavorativa è fortemente sconsigliato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza ed è ammesso solo in presenza di gravi motivi personali. Il Personal Computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

3.2 Il Personal Computer dato in affidamento all'utente permette l'accesso alla rete dell'Istituto Scolastico solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 4 del presente Regolamento.

3.3 L'Istituto Scolastico rende noto che il personale incaricato è stato autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware etc.).
Detti interventi potranno anche comportare l'accesso, in caso di importanti esigenze operative o di eventi dannosi o di situazioni di pericolo, con congruo preavviso all'utente ed alla presenza di quest'ultimo o di un suo fiduciario opportunamente delegato in forma scritta, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Istituto, si applica anche in caso di assenza prolungata od impedimento dell'utente.

3.4 Il personale autorizzato ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

3.5 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone l'Istituto Scolastico a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore (impongono la presenza nel sistema di software regolarmente licenziati o comunque liberi e quindi non protetti dal diritto d'autore) vengono sanzionate anche penalmente.

3.6 Salvo preventiva espressa autorizzazione, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere all'installazione di dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem).

3.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Responsabile del Trattamento nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 10 del presente Regolamento relativo alle procedure di protezione antivirus.

3.8 Il Personal Computer deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. 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.

4. Gestione ed assegnazione delle credenziali di autenticazione

4.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal Titolare del Trattamento.

4.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), associato ad una parola chiave (password) riservata che dovrà essere custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione, senza preventiva autorizzazione da parte del Titolare del Trattamento.

4.3 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

4.4 È necessario procedere alla modifica della parola chiave, a cura dell'utente incaricato del trattamento, al primo utilizzo e successivamente almeno ogni sei mesi (ogni tre mesi nel caso di trattamento dei dati sensibili attraverso l'ausilio di strumenti elettronici).

4.5 Qualora fosse necessaria la sostituzione della parola chiave, per decorrenza del termine sopraindicato e/o in seguito alla perdita della propria riservatezza, si procederà in tal senso.

4.6 Soggetto preposto alla custodia delle credenziali di autenticazione è Titolare del Trattamento.

5. Utilizzo della rete dell'Istituto Scolastico

5.1 Per l'accesso alla rete ciascun utente deve essere in possesso delle specifiche credenziali di autenticazione.

5.2 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'accesso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

5.3 Le cartelle utenti presenti nei server sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file non inerente 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 da parte del Titolare del Trattamento.

5.4 Il Titolare del Trattamento può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà pericolosi per la Sicurezza sulle unità di rete.

5.5 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6. Utilizzo e conservazione dei supporti rimovibili

6.1 Tutti i supporti magnetici rimovibili (CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

6.2 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il Titolare e seguire le istruzioni da questi impartite.

6.3 In ogni caso, i supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dagli utenti, in armadi chiusi.

6.4 E' vietato l'utilizzo di supporti rimovibili personali.

6.5 L'utente è responsabile della custodia dei supporti e dei dati istituzionali in essi contenuti.

7. Utilizzo di PC portatili

7.1 L'utente è responsabile del PC portatile assegnatogli dal Titolare del Trattamento e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

7.2 Ai PC portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

7.3 I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

8. Uso della posta elettronica

8.1 La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

8.2 È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche (o "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al Titolare del Trattamento. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

8.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

9. Navigazione in Internet

9.1 Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

9.2 In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:
- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione;
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- 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) se non espressamente autorizzati dal Responsabile d'ufficio;
- l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

9.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Istituzione scolastica rende nota, peraltro, l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list.

9.4 Gli eventuali controlli, compiuti dal Titolare del Trattamento ai sensi del precedente punto 3.3, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log".
In applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet ed al traffico telematico (log di sistema e del server proxy), la cui conservazione non sia necessaria, saranno cancellati entro tre mesi dalla loro produzione, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'amministrazione.

In casi eccezionali (es.: esigenze tecniche o di sicurezza; indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria; obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria) è consentito il prolungamento dei tempi di conservazione limitatamente al soddisfacimento delle esigenze sopra esplicitate.

10. Protezione antivirus

10.1 Il sistema informatico della scuola è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

10.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al Titolare del Trattamento.

10.3 Ogni dispositivo magnetico di provenienza esterna all'Istituzione dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al Titolare del Trattamento.

11. Utilizzo dei telefoni, fax e fotocopiatrici aziendali

11.1 Gli apparecchi telefonici sono strumenti di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa.

11.3 È vietato l'utilizzo dei fax per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di ufficio.

11.4 È vietato l'utilizzo delle fotocopiatrici per fini personali.

12. Osservanza delle disposizioni in materia di Privacy

12.1 È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione ad autorizzato del trattamento dei dati ai sensi D.Lgs. n. 196/2003 e del Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

13. Aggiornamento e revisione

13.1 Il presente Regolamento è soggetto a revisione con frequenza annuale.