REGOLAMENTO INTERNO SULL'USO DEI SISTEMI ELETTRONICI E INFORMATICI

INDICE

PREMESSA

Le prescrizioni e le indicazioni che seguiranno si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli "autorizzati al trattamento" in conformità al regolamento generale sulla protezione dei dati dell'UE 679/2016 (GDPR).
Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione del presente Regolamento è possibile rivolgersi al Titolare del trattamento, o al Responsabile per la protezione dei dati personali (DPO).

SCOPO E AMBITO DI APPLICAZIONE

Il presente documento ha l'obiettivo di fornire indicazioni relative alla produzione, gestione, trasmissione e conservazione dei dati personali con particolare attenzione a quelle di tipo elettronico che, per loro natura, risultano particolarmente critiche.

Il presente documento è destinato al personale dipendente dell'**I.P.S.S.E.C. "A. OLIVETTI" "**Dipendenti"), ai suoi collaboratori in qualità di consulenti esterni o altre forme similari di collaborazione ("Utenti") che utilizzano strumenti informatici o che sono interessati al trattamento. In generale i contenuti devono essere noti a tutti coloro che gestiscono informazioni appartenenti all'istituto o di terzi che intrattengono rapporti con l'istituto.

RIFERIMENTI NORMATIVI E DOCUMENTALI

NORMATIVA

- ***GDPR**, regolamento 2016/679 del Parlamento europeo e del Consiglio dell'Unione Europea relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*

- ***Decreto Legislativo 30 giugno 2003, n. 196 e successive integrazioni e modificazioni** ("Codice in materia di protezione dei dati personali")*

- ***Decreto Legislativo 8 giugno 2001, n. 231,** recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300", pubblicato in
Gazzetta Ufficiale n. 140 del 19 giugno 2001, e successive modificazioni e integrazioni.*

- ***Legge 20 maggio 1970, n. 300**, norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e nell'attività sindacale nei luoghi di lavoro e norme sul collocamento (detta anche "statuto dei lavoratori")*

PROVVEDIMENTI AUTORITA' GARANTE PRIVACY

- **Linee Guida del Garante Privacy su Posta Elettronica e Internet** (Deliberazione n. 13 del 1 marzo 2007 – G.U. n. 58 del 10 marzo 2007)

- **Provvedimento del Garante Privacy del 27 novembre 2008** e successive modificazioni relativo a "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

- **Vademecum "Privacy e Lavoro** - Le regole per il corretto trattamento dei dati personali dei lavoratori da parte di soggetti pubblici e privati", del 24 aprile 2015

DOCUMENTI INTERNI

- **"programmazione delle misure di sicurezza nel trattamento dei dati personali"**

NORME COMPORTAMENTALI GENERALI

Le principali norme comportamentali sono elencate di seguito:

Rispetto della Legislazione

Ai sensi del regolamento generale sulla protezione dei dati dell'UE 679/2016 (GDPR), è considerato dato personale qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Le tre tipologie di dato personale sono le seguenti:

- Dati personali semplici;
- Dati particolari, ovvero dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- dati giudiziari, ovvero i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Per trattamento dei dati si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

È proibito utilizzare il sistema informatico in violazione della legislazione vigente, delle istruzioni del Titolare del trattamento e comunque per motivi estranei alle mansioni affidate da quest'ultimo in virtù del rapporto contrattuale in essere.

Per prevenire eventuali utilizzi illeciti, l'istituto, attraverso funzione responsabile dei sistemi informatici (c.d. "Responsabile IT" o "Amministratore di sistema"), si riserva la facoltà di effettuare saltuariamente dei controlli a campione circa l'utilizzo di tali apparecchiature fatto da ciascun Dipendente o Utente.

1. GESTIONE DELLE CREDENZIALI DI ACCESSO

Le credenziali di accesso sono composte da una coppia nome utente e password che identificano uno specifico Utente, il quale sarà ritenuto responsabile di ogni operazione effettuata attraverso il loro uso, anche da parte di terzi. E' quindi cura di ogni utente garantire la riservatezza delle credenziali assegnate.
L'accesso al personal computer deve essere sempre protetto con le credenziali di accesso e questa deve essere custodita dall'incaricato con la massima diligenza e per nessuna ragione dovrà essere divulgata.

2. UTILIZZO DEL PERSONAL COMPUTER

Il personal computer affidato al Dipendente o all'Utente è uno **strumento di lavoro.** Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

La funzione responsabile dei sistemi informatici, per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno.

Tale funzione aziendale potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere all'istituto (titolare del trattamento), ai fini privacy, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa e al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività lavorativa nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente quest'ultimo dell'intervento di accesso realizzato.

3. TRATTAMENTO DEI DATI INFORMATICI

3.1 Trattamento di dati personali, compresi quelli che contengono informazioni di tipo particolare e/o giudiziario, generati o contenuti dai sistemi informatici interni

E' consentito:

- Trattare, secondo il proprio profilo di autorizzazione (permessi), i dati personali contenuti negli archivi elettronici, cartacei e informatici di proprietà del Titolare del trattamento, la cui conoscenza è necessaria e sufficiente per lo svolgimento dei compiti affidati da quest'ultimo.

E' vietato:

- effettuare trattamenti al di fuori dei limiti imposti dal proprio profilo di autorizzazione (permessi) e in maniera difforme dalle istruzioni del Titolare del trattamento;

- comunicare a terzi i dati personali trattati, salvo che la comunicazione sia indispensabile per lo svolgimento delle proprie mansioni e avvenga nei confronti di terzi autorizzati dal Titolare del trattamento, oppure avvenga nei confronti di organi giurisdizionali, o avvenga nell'adempimento di obblighi di legge, di regolamenti, di provvedimenti delle Autorità, fatta salva, in ogni caso, diversa istruzione del Titolare del trattamento;

3.2 Attività di controllo

Il responsabile dei sistemi informatici può in qualunque momento procedere alla rimozione di ogni file che riterrà essere pericoloso per la sicurezza sulle unità di rete. In tal caso, il Titolare del trattamento, per garantire la piena sicurezza della Rete o per motivi di manutenzione, si riserva di superare ogni accesso e limitazione predisposta (ad esempio password, E-Mail, dischi di rete).

4. USO DELLA POSTA ELETTRONICA

La casella di posta, assegnata al Dipendente e all'Utente, è uno **strumento di lavoro**. L'account assegnato non è personale (ad uso esclusivo dell'assegnatario), ma unicamente personalizzato (ad uso lavorativo e identificativo dell'assegnatario), di conseguenza si tratta di un bene di proprietà dell'istituto. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Le caselle di posta elettronica date in uso al Dipendente o all'Utente, pertanto, sono destinate ad un utilizzo esclusivamente lavorativo.

4.1 Linee guida generali sulla posta elettronica

Ogni Dipendente o Utente, in caso di assenza per qualsiasi motivo (ferie, allontanamento temporaneo dal posto di lavoro, malattia) e al fine di non interrompere né rallentare i processi lavorativi, ha la facoltà di inserire nel proprio account di posta elettronica la funzione di risposta automatica, contenente eventualmente le coordinate di altri lavoratori a cui rivolgersi in sua sostituzione; il delegato potrà in questo modo ricevere i messaggi di posta elettronica del Dipendente o Utente assente e a lui indirizzati.
In caso di assenza prolungata dell'incaricato l'istituto, anche per il tramite di soggetto all'uopo nominato (amministratori di sistema), potrà accedere all'account di posta elettronica, al fine di verificare il contenuto di messaggi e utilizzare quelli utili per il regolare svolgimento dell'attività lavorativa.

5. UTILIZZO DEI DISPOSITIVI PORTATILI

I dispositivi portatili, intesi come tutti i dispositivi che sono o che possono essere spostati con facilità al di fuori dei locali dall'istituto per esigenze lavorative quali laptop, tablet, smartphone, ecc.., devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni. La caratteristica della portabilità, infatti, rappresenta nel contempo il punto di forza e di debolezza in quanto, seppur di piccole dimensioni, questi moderni dispositivi possono contenere quantità rilevanti di dati personali.

Nel caso in cui i dispositivi portatili siano utilizzati al di fuori dei locali scolastici e abbiano accesso ai dati dell'istitituto, il trattamento degli stessi dovrà essere effettuato secondo le linee guida indicate nel punto 3 del regolamento.

Ai dispositivi portatili si applicano le regole di utilizzo previste al punto 2 sull'utilizzo del personal computer.

6. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

La rete Internet rappresenta una risorsa fondamentale e il suo utilizzo da parte dei Dipendenti e Utenti è essenziale per il corretto svolgimento di tali attività. Nel contempo però tale risorsa può rappresentare anche una minaccia per la sicurezza dei dati dell'istituto o dei suoi studenti. Infatti nell'underground tecnologico di Internet si possono incontrare facilmente (tramite la semplice navigazione o il download di file) minacce che possono compromettere la riservatezza e la disponibilità dei dati personali (si parla di Malware in generale, ma anche di pagine web infette come veicolo di tale software malevolo).

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.

E' fatto anche divieto al Dipendente e all'Utente di scaricare software gratuiti (freeware) e shareware prelevati da siti internet, etc., salvo precisa indicazione o autorizzazione del proprio superiore di riferimento.

6.1 Modalità di controllo e prevenzione di utilizzo illecito

L'istituto, al fine di prevenire determinate operazioni non consentite, ha implementato misure di sicurezza che puntano a mitigare i rischi sopra esposti; ma la prima e più efficace misura di sicurezza è rappresentata dalla consapevolezza del Dipendete e dell'Utente. Comunque, nel caso in cui un evento dannoso o una situazione di pericolo non siano stati impediti con preventivi accorgimenti tecnici, l'istituto adotterà eventuali misure che consentano la verifica di comportamenti anomali, attraverso le modalità e le procedure di seguito specificate (punto 11).

7. UTILIZZO DEL FAX, TELEFONO, FOTOCOPIATRICI E DELLA DOCUMENTAZIONE CARTACEA

Il fax, il telefono e le fotocopiatrici devono essere utilizzati per scopi puramente lavorativi.

Non è consentito rivelare numeri telefonici interni o informazioni dell'istituto o dati in suo possesso a persone non preventivamente e positivamente identificate ed è fatto divieto di lasciare documenti incustoditi presso le postazioni di fax o presso i locali delle fotocopiatrici.

8. FORMAZIONE

La prima misura di sicurezza per la protezione dei dati personali è indubbiamente la preparazione e consapevolezza dei Dipendenti e degli Utenti nello svolgere il proprio lavoro in modo sicuro.

Consapevolezza e preparazione sono aspetti che fanno parte del background del Dipendente e dell'Utente ma che possono essere sviluppati anche attraverso specifica formazione nelle varie fasi della vita lavorativa (corsi di inserimento e di aggiornamento periodico).

In ambito sicurezza delle informazioni e Privacy si fa obbligo di partecipare alle attività di formazione e aggiornamento predisposte dal Titolare del trattamento.

9. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

E' obbligatorio attenersi alle disposizioni in materia di Privacy, nonché in materia di misure idonee di sicurezza.

I consulenti o collaboratori esterni si obbligano al rispetto degli obblighi indicati nei contratti sottoscritti con l'istituto e che ne disciplinano i rapporti con lo stesso. Nei casi di maggior gravità, dovuti a inosservanza del presente regolamento e degli obblighi contrattuali assunti in materia di privacy e riservatezza, si specifica che dopo il secondo richiamo formale sarà applicata la clausola risolutiva espressa (se prevista), salvo l'eventuale richiesta di risarcimento danni.

10. CONTROLLI

L'istituto si riserva la facoltà, nel rispetto della tutela del diritto alla riservatezza e del principio di proporzionalità e non eccedenza, di svolgere dei controlli difensivi e/o indiretti che consentano di verificare l'effettiva conformità dell'uso degli strumenti informatici alle presenti prescrizioni.

Tali controlli saranno effettuati secondo un meccanismo progressivo, partendo da controlli a campione e anonimi, per poi, qualora si rilevassero delle anomalie, passare a controlli più puntuali e diretti all'individuazione dei singoli trasgressori.

11. VIDEOSORVEGLIANZA

La Società fa presente che presso la propria sede è presente un sistema di videosorveglianza – con telecamere poste nella aree esterne e interne (accesso alle sedi dell'azienda, uscite di sicurezza, etc.) - finalizzato alla protezione del patrimonio mobiliare e immobiliare, degli accessi e di particolari aree sensibili. In ogni caso, le telecamere non riprendono in maniera diretta l'ambiente lavorativo ed esclusa qualsiasi attività di controllo diretto del lavoratore. Per maggiori precisazioni si rimanda alla specifica informativa in tema di videosorveglianza.

12. NON OSSERVANZA DELLA NORMATIVA INTERNA E PROVVEDIMENTI DISCIPLINARI

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento sono perseguibili con provvedimenti disciplinari nonché, nei casi più gravi, con azioni civili e penali.

Nei casi di accertata violazione delle norme di comportamento fissate nel presente documento o comunque portate a conoscenza dei Dipendenti e degli Utenti è prevista l'applicazione dei provvedimenti disciplinari di seguito individuati o l'applicazione delle specifiche sanzioni previste nelle clausole contrattuali per i soggetti non dipendenti.

A seconda della gravità della violazione perpetrata la sanzione disciplinare prevista può prevedere:
- un semplice richiamo verbale;
- l'applicazione della multa;
- la risoluzione immediata del rapporto di lavoro instaurato (giusta causa).

La non osservanza del presente regolamento e delle disposizioni interne può comportare, oltre alle sanzioni disciplinari, anche sanzioni civili e penali.

Si precisa inoltre che, ai fini disciplinari, le presenti disposizioni e procedure operative interne, sono affisse in luoghi accessibili a tutti (es. bacheca aziendale), ai sensi dell'art. 7 della Legge 20 maggio 1970 n. 300.

I Dipendenti e gli Utenti, qualora venissero a conoscenza di violazioni da parte dei Colleghi ai comportamenti di cui ai punti precedenti, hanno l'obbligo di denunciare immediatamente l'accaduto ai responsabili competenti.

AGGIORNAMENTO E REVISIONE

Il presente regolamento è soggetto a revisione con frequenza annuale ovvero può essere modificato in base all'entrata in vigore di nuove prescrizioni di legge in ambito comunitario o nazionale.

Qualora l'istituto intenda apportare modifiche al presente regolamento, queste saranno applicate dandone conoscenza immediata a tutti i destinatari mediante apposita circolare di servizi e affissione alla bacheca comune.

La Direzione

_____

REVISIONI			
N°	**MOTIVI**	**DATA**	**NOME**
1			
2			