ISTITUTO COMPRENSIVO "SAN GIOVANNI BOSCO"
71043 M A N F R E D O N I A – F G
Via Cavolecchia, 4 – CF: 92055050717 – CM: FGIC872002
Codice Univoco ufficio (CUU): UF6AFD - Codice iPA: istsc_fgic86700e
Tel.: 0884585923 Fax: 0884516827
Sito Web: www.icsangiovannibosco.edu.it
PEO: fgic872002@istruzione.it – PEC: fgic872002@pec.istruzione.it

DISCIPLINARE UTILIZZO DI INTERNET

Approvato dal Consiglio d'Istituto in data ///

Rispetto all'utilizzo interno delle strumentazioni informatiche, della rete internet e della posta elettronica da parte del personale docente, non docente e degli studenti, tenendo conto che:

1. *compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;*
2. *spetta ad essi adottare idonee misure di sicurezza, per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possano essere fonte di responsabilità (art. 15 - 31 ss., 167 e 169 del Codice);*
3. *emerge l'esigenza di tutelare i lavoratori interessati e gli studenti, anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un ulteriore rapido incremento;*
4. *considerando che il Garante per la protezione dei dati personali, emanando le linee guida pubblicate sulla Gazzetta Ufficiale n.58 del10 marzo 2007, ha ritenuto opportuno ascrivere ai datori di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali sono le modalità di utilizzo degli strumenti a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati eventuali controlli*

viene disposto il seguente disciplinare

Compete al datore di lavoro:

- *assicurare la funzionalità delle dotazioni informatiche in dotazione all'istituto*
- *adottare idonee misure di sicurezza, per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, nonché per prevenire utilizzi indebiti*
- *adottare limiti e cautele per evitare la registrazione e la diffusione di fotografie e filmati, in tempo reale, anche utilizzando i terminali di nuova generazione, applicati alla telefonia mobile*
- *indicare in modo particolareggiato quali siano gli strumenti messi a disposizione e le modalità di utilizzo da parte dei dipendenti ritenute corrette, nell'organizzazione dell'attività lavorativa*
- *precisare in che misura e con quali modalità vengano effettuati i controlli*
- *tutelare i lavoratori interessati nel trattamento di dati per finalità di gestione del rapporto in ambito pubblico, adottando quelle misure che garantiscono un elevato standard di sicurezza e garanzia*
- *tener conto della normativa, illustrata nel presente disciplinare, per come di seguito riportata che si aggiunge ed integra le specifiche istruzioni già fornite a tutti gli incaricati del trattamento dati in attuazione del G.D.P.R. e a cui devono attenersi tutti gli utilizzatori (d'ora in poi definiti utenti) delle strumentazioni informatiche, della rete internet e della posta elettronica*

Il presente Regolamento disciplina le modalità di accesso e di uso della Rete Informatica, telematica e dei servizi che, tramite la rete stessa, è possibile ricevere o offrire all'interno e all'esterno dell'istituto per dare il supporto informativo documentario alla ricerca, alla didattica, all'aggiornamento e alle attività collaborative tra scuola ed enti, nonché per tutti gli adempimenti amministrativi di legge.

La rete dell'istituto è costituita dall'insieme delle Risorse informatiche, cioè

- *dalle componenti hardware/software e dagli apparati elettronici collegati alla Rete informatica dell'istituto*
- *dall'insieme delle banche dati in formato digitale ed in generale di tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati*

Il presente regolamento si applica, senza distinzione di ruolo e/o livello, a tutti gli utenti interni (personale amministrativo, docenti e collaboratori scolastici), autorizzati ad accedere alla rete della scuola nell'ambito della propria attività lavorativa ordinaria e straordinaria, e agli studenti nei limiti loro assegnati a scopi didattici ed educativi.

Analogamente il presente regolamento si applica al personale, anche esterno, che effettua attività di manutenzione e agli altri eventuali soggetti esterni autorizzati all'accesso a specifiche banche dati e a tutti i collaboratori dell'istituto, a prescindere dal rapporto contrattuale con gli stessi intrattenuto (es. soggetti in attività di stage, relatori e formatori per corsi di aggiornamento).

L'istituto prevede l'utilizzo delle strumentazioni informatiche, della rete internet e della posta elettronica, da parte degli utenti, quali strumenti utili a perseguire le proprie finalità istituzionali e prevede che lo stesso si conformi ai seguenti principi:

- *principio di necessità: i sistemi informativi e i programmi informatici vengono configurati, riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in relazione alle finalità perseguite;*
- *principio di correttezza: le caratteristiche essenziali dei trattamenti sono rese note ai lavoratori*
- *principio di pertinenza e non eccedenza: i trattamenti sono effettuati per finalità determinate, esplicite e legittime e i dati sono trattati nella misura meno invasiva possibile.*

La Rete informatica di istituto, l'accesso alla rete internet e alla posta elettronica, il Pc affidato al dipendente sono strumenti di lavoro; su di essi vengono effettuate regolari attività di controllo, amministrazione e back up ed essi non possono in alcun modo essere utilizzati per scopi diversi perché ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

In relazione all'utilizzo non corretto dei citati strumenti si individuano i possibili rischi e conseguenti effetti, rappresentati nella tabella sottostante:

Attività	*Rischi*	*Motivazione*	*Possibile effetto*
Manutenzione di periferiche hardware interne (scheda video, ecc.)	*Alto*	*Possono essere danneggiati componenti interne e il PC*	
Manutenzione di periferiche hardware esterne (tastiera, mouse, ecc.)	*Basso*		
Download non controllato o non programmato di aggiornamenti relativi ad applicazioni installate dal responsabile di rete	*Alto*	*Possono essere scaricate applicazioni non verificate con il pericolo di portare Virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore*	*Danneggiamento del software del PC o della rete informatica interna*
Download controllato o programmato di aggiornamenti relativi ad applicazioni installate dal responsabile di rete	*Basso*		

Download di dati non inerenti alle attività lavorative (musica, giochi, ecc.)	*Alto*	*Possono essere scaricate applicazioni non verificate con il pericolo di portare virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore*	*Danneggiamento del software del PC o della rete informatica interna.* *Gravi responsabilità civili e penali per l'istituto in caso di violazione della normativa a tutela dei diritti d'autore.*
Installazione di applicazioni senza l'autorizzazione del responsabile della rete	*Alto*	*Possono essere installate applicazioni non compatibili*	*Danneggiamento del software del PC o della rete informatica interna*
Accesso alla rete effettuato da Pc di proprietà dell'utente	*Alto*	*Accessi non autorizzati alla rete*	*Furto di dati*
Download delle e- mail	*Medio/ Alto*		
Apertura di allegati di posta elettronica di incerta provenienza	*Alto*	*Contenere Malware/Spyware*	*Danneggiamento del software del PC o della rete informatica interna.* *Divulgazione di password e dati riservati*
Elaboratore connesso alla rete lasciato incustodito o divulgazione di password	*Alto*	*Possibile utilizzo da parte di terzi*	*Uso indebito di dati riservati, danneggiamento della rete informatica interna.*
Utilizzo di supporti removibili esterni non autorizzati	*Alto*	*Possono essere trasferite applicazioni dannose per il PC nella rete informatica*	*Danneggiamento dei PC o della rete informatica interna. Furto di dati*
Mancata distruzione o perdita accidentale di supporti magnetici riutilizzabili (dischetti,nastri,DAT,chiavi usb, cdriscrivibili...)contenenti dati sensibili e giudiziari	*Alto*	*Recupero di dati memorizzati anche dopo la loro cancellazione*	*Uso indebito di dati riservati*

Per ridurre il rischio di impieghi abusivi o dannosi, il datore di lavoro provvede a:

- *individuare preventivamente le postazioni di lavoro e assegnarle personalmente a ciascun dipendente*
- *individuare preventivamente gli utenti a cui è accordato l'accesso a internet.*

La strumentazione dell'istituto non è di esclusivo dominio del dipendente, ma rientra tra i beni, a cui determinati soggetti possono comunque sempre accedere. L'eventuale accesso del datore di lavoro, qualora necessiti di informazioni contenute nei documenti, residenti sul PC assegnato al dipendente, è legittimo.

Il datore di lavoro conferisce all'amministratore di sistema il compito di sovrintendere alle risorse informatiche dell'istituto assegnandogli in maniera esclusiva le seguenti attività:

- *gestione dell'hardware e del software (installazione, aggiornamento, rimozione) di tutte le strutture tecniche informatiche dell'istituto, siano esse collegate in rete o meno*
- *configurazione dei servizi di accesso alla rete interna, ad internet e a quelli di posta elettronica con creazione, attivazione e disattivazione dei relativi account*
- *attivazione della password di accensione e/o di accesso ai pc*
- *creazione di un'area condivisa sul server per lo scambio dei dati tra i vari utenti, evitando condivisioni dei dischi o di altri supporti configurati nel PC che non siano strettamente necessarie perché sono un ottimo "aiuto" per i software che cercano di "minare" la sicurezza dell'intero sistema*
- *controllo del corretto utilizzo delle risorse di rete, dei computer e degli applicativi, durante le normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori*
- *rimozione sia sui PC degli incaricati sia sulle unità di rete, di ogni tipo di file o applicazione che può essere pericoloso per la sicurezza o costituisce violazione del presente regolamento*
- *cancellazione delle unità di memoria interne alla macchina (hard - disk, memorie allo stato solido) ogni qualvolta si procederà alla dismissione di un PC e dei supporti removibili consegnati a tale scopo dagli utenti*
- *utilizzo delle credenziali di amministrazione del sistema per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di indispensabile ed indifferibile necessità di intervento per prolungata assenza, irrintracciabilità o impedimento dello stesso, ma solo per il tempo necessario al compimento di attività indifferibili e solo su richiesta del Responsabile del trattamento, fermo restando che l'amministratore di sistema, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, ha facoltà di accedere in qualunque momento, anche da remoto, e dopo aver informato l'utente interessato, al PC di ciascun utente.*

Per l'accesso alla strumentazione informatica di istituto ciascun utente deve essere in possesso delle specifiche credenziali di autenticazione, previste ed attribuite dall'incaricato della custodia delle password.

Le credenziali di autenticazione per l'accesso alla rete e/o alle macchine vengono assegnate dal custode delle password e 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 può essere divulgata.

- *è necessario procedere alla modifica della parola chiave, a cura dell'incaricato, al primo utilizzo. Se l'utente non provvede autonomamente a variare la password entro i termini massimi, viene automaticamente disabilitato. Provvederà l'amministratore di sistema a riabilitare l'utente e ad assegnargli una password provvisoria che l'utente dovrà cambiare al primo accesso*
- *per scegliere una parola chiave si devono seguire le istruzioni fornite dall'amministratore di sistema.*
- *la password deve essere cambiata a intervalli regolari a cura dell'incaricato del trattamento d'intesa con il custode della password*
- *la variazione delle password deve essere comunicata al custode delle password a cui dovrà essere consegnata in busta chiusa con data e firma dell'incaricato apposte sul lembo di chiusura, perché ne curi la conservazione*
- *è necessario curare la conservazione della propria parola chiave e bisogna evitare di comunicarla ad altri, di trascriverla su supporti (agenda, post-it,..) che siano accessibili ad altri o di consentire che qualcuno sbirci quello che si sta scrivendo sulla tastiera quando viene immessa la password*

- *nel caso si sospetti che la password abbia perso la segretezza essa deve essere immediatamente sostituita, dandone comunicazione al custode delle password*

La navigazione in internet costituisce uno strumento necessario allo svolgimento delle attività lavorative e didattiche. L'accesso ad Internet è regolato da filtri predefiniti dall'amministratore di sistema su autorizzazione dell'amministrazione, con esclusione dei siti istituzionali.

Il titolare del trattamento provvede alla individuazione delle categorie di siti considerati correlati o non correlati con la prestazione lavorativa.

La rete informatica permette di salvare su server i files relativi alla produttività individuale. Le aree di condivisione in rete sono soggette a regolari attività di controllo, amministrazione e back-up. L'accesso è regolamentato da policies di sicurezza che suddividono gli accessi fra gruppi e utenti. Periodicamente si provvede alla pulizia degli archivi, con cancellazione dei files obsoleti ed inutili

L'amministratore di sistema provvede alla configurazione di sistemi e all'utilizzo di filtri che prevengono determinate operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di file o software).

Per assicurare la tutela dei diritti, delle libertà fondamentali e della dignità dei lavoratori, garantendo che sia assicurata una ragionevole protezione delle loro sfera di riservatezza nelle relazioni personali professionali, il trattamento dei dati mediante l'uso delle tecnologie telematiche è conformato al rispetto dei diritti delle libertà fondamentali nonché della dignità dell'interessato, dei divieti posti dallo statuto dei lavoratori sul controllo a distanza e dei principi di necessità, correttezza e finalità determinate, esplicite e legittime.

Ogni utente è responsabile, sia sotto il profilo civile che penale, del corretto uso delle risorse informatiche, dei servizi e dei programmi ai quali ha accesso e dei dati che tratta.

Spetta ai docenti vigilare affinché gli studenti loro affidati rispettino il presente regolamento.

Le strumentazioni informatiche, la rete internet e la posta elettronica devono essere utilizzate dal personale e dagli studenti sotto il controllo dei loro docenti, come strumenti di lavoro e studio.

Ogni loro utilizzo non inerente l'attività lavorativa e di studio è vietato in quanto può comportare disservizi, costi di manutenzione e soprattutto minacce alla sicurezza.

In particolare non può essere dislocato nelle aree di condivisone della rete alcun file che non sia legato all'attività lavorativa, nemmeno per brevi periodi.

Agli utenti è severamente vietata la memorizzazione di documenti informatici di natura oltraggiosa o discriminatoria per sesso, lingua, religione, razza, origine etnica, condizioni di salute, opinioni, appartenenza sindacale politica.

Non è consentito scaricare, scambiare o utilizzare materiale coperto dal diritto d'autore.

Gli utenti utilizzano per il proprio lavoro soltanto computer di proprietà dell'istituto, salvo espresse autorizzazioni contrarie dell'amministratore di sistema e sono tenuti a:

- *attivare sul PC lo screen saver e la relativa password*
- *conservare la password nella massima riservatezza e con la massima diligenza*
- *non inserire password locali che non rendano accessibile il computer agli amministratori di rete se non esplicitamente autorizzato dal servizio informatico dell'istituto*
- *non utilizzare cripto sistemi o qualsiasi altro programma di sicurezza crittografa non previsti esplicitamente dal servizio informatico dell'istituto*
- *non modificare la configurazione hardware e software del proprio PC se non esplicitamente autorizzati dall'amministratore di sistema*
- *non rimuovere, danneggiare o asportare componenti hardware*
- *non installare sul proprio PC dispositivi hardware personali (modem, schede audio, masterizzatori, pendrive, dischi esterni, i-pood, telefoni, ecc.), fatta salva specifica autorizzazione in tal senso da parte del responsabile*
- *non installare autonomamente programmi informatici, se non esplicitamente autorizzati dall'amministratore di sistema*
- *non utilizzare programmi non autorizzati, con particolare riferimento ai videogiochi che sono portatori utilizzati , per veicolare virus*
- *mantenere sempre aggiornati e attivi sulla propria postazione di lavoro i software antivirus con riferimento all'ultima versione disponibile*
- *nel caso in cui il software antivirus rilevi la presenza di un virus, sospendere immediatamente ogni elaborazione in corso, senza spegnere il PC e segnalare prontamente l'accaduto al personale incaricato dell'assistenza tecnica*
- *prestare la massima attenzione ai supporti di origine esterna (es. pendrive), verificando preventivamente tramite il programma antivirus ogni file acquisito attraverso qualsiasi supporto e avvertendo immediatamente l'amministratore di sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti*
- *non lasciare incustodita e accessibile la propria postazione, una volta connessi al sistema con le proprie credenziali di autenticazione*
- *non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a persone non autorizzate, in particolar modo per quanto riguarda l'accesso ad internet e ai servizi di posta elettronica*
- *spegnere il PC al termine del lavoro o in caso di assenze prolungate dalla propria postazione.*

Gli utenti della rete informatica sono tenuti a utilizzare la rete in modo conforme a quanto stabilito dal presente regolamento e quindi:

- *mantenere segrete e non comunicare a terzi, inclusi gli amministratori di sistema, le password d'ingresso alla rete ed ai programmi e non permettere ad alcuno di utilizzare il proprio accesso*
- *provvedere periodicamente alla pulizia degli archivi con cancellazione dei file obsoleti o inutili ed evitare un'archiviazione ridondante*
- *verificare preventivamente ogni archivio elettronico (file) acquisito attraverso qualsiasi supporto (es. pendrive) prima di trasferirlo su aree comuni della rete*

Agli utenti è fatto espresso divieto di influenzare negativamente la regolare operatività della rete, interferendo con la connettività altrui o con il funzionamento del sistema e quindi di:

- *utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files o software di altri utenti, utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di intercettazione di tastiera (keygrabber o keylogger), software di decodifica password (cracker) e più in generale software rivolti alla violazione della sicurezza del sistema e delle privacy*
- *sostituirsi a qualcuno nell'uso dei sistemi, cercare di catturare password altrui o forzare password o comunicazioni criptate*
- *modificare le configurazioni impostate dall'amministratore di sistema*
- *limitare o negare l'accesso al sistema a utenti legittimi*
- *effettuare trasferimenti non autorizzati di informazioni (software, dati,..)*
- *distruggere o alterare dati altrui*
- *usare l'anonimato o servirsi di risorse che consentano di restare anonimi*

L'accesso alla navigazione in internet deve essere effettuato esclusivamente a mezzo della rete di istituto e solo per fini lavorativi o di studio. È tassativamente vietato l'utilizzo di modem personali. Gli utenti sono tenuti ad utilizzare l'accesso ad internet in modo conforme a quanto stabilito dal presente regolamento e quindi devono:

- *navigare in internet in siti attinenti allo svolgimento delle mansioni assegnate*
- *registrarsi solo a siti con contenuti legati all'attività lavorativa*
- *partecipare a forum o utilizzare chat solo per motivi strettamente attinenti l'attività lavorativa*

Agli utenti è fatto espresso divieto di qualsiasi uso di internet che possa in qualche modo recare danno all'istituto o a terzi e quindi di:

- *fare conoscere ad altri la password del proprio accesso, inclusi gli amministratori di sistema*
- *usare internet per motivi personali*
- *servirsi dell'accesso internet per attività in violazione del diritto d'autore o di altri diritti tutelati dalla normativa vigente*
- *accedere a siti pornografici, di intrattenimento,..*
- *scaricare i software gratuiti dalla rete, salvo casi di comprovata utilità e previa autorizzazione in tal senso da parte del responsabile*
- *utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer*
- *ascoltare la radio o guardare video o filmati, utilizzando le risorse internet*
- *effettuare transazioni finanziarie, operazioni di remote banking, acquisti online e simili, se non attinenti l'attività lavorativa o direttamente autorizzati dal responsabile del trattamento*
- *inviare fotografie, dati personali o di amici dalle postazioni internet*

Nell'uso della posta elettronica istituzionale gli utenti autorizzati sono responsabili del corretto utilizzo della stessa e sono tenuti a utilizzarla in modo conforme a quanto stabilito dal presente regolamento, quindi devono:

- *conservare la password nella massima riservatezza e con la massima diligenza*
- *utilizzare tecniche per l'invio di comunicazioni a liste di distribuzione solo se istituzionali*
- *inoltrare, a chi di riferimento nell'istituto, ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali con l'istituto e fare riferimento alle procedure in essere per la corrispondenza ordinaria*

- *utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta ricezione del messaggio da parte del destinatario*
- *prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura e, dove possibile, preferire l'utilizzo di cartelle di rete condivise*
- *inviare preferibilmente file in formato PDF*
- *accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i file attachment di posta elettronica prima del loro utilizzo*
- *rispondere a e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre*
- *chiamare link contenuti all'interno di messaggi solo quando vi sia la comprovata sicurezza sul contenuto dei siti richiamati*

Agli utenti è fatto divieto di qualsiasi uso della posta elettronica che possa in qualche modo recare danno all'istituto o a terzi e quindi di:

- *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*
- *inviare tramite posta elettronica user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici*
- *utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing list salvo diversa ed esplicita autorizzazione*
- *inviare o ricevere posta personale attraverso l'uso di un webmail*
- *inviare o accettare messaggi in formato html*
- *utilizzare il servizio di posta elettronica per inoltrare giochi, scherzi, barzellette, appelli e petizioni, messaggi tipo "catene" e altre e-mail che non siano di lavoro*

Gli utenti devono trattare con particolare cura i supporti magnetici (dischetti, nastri, DAT, chiavi USB, CD riscrivibili,..) in particolar modo quelli riutilizzabili, per evitare che persone non autorizzate possano accedere ai dati ivi contenuti e quindi devono:

- *non utilizzare supporti rimovibili personali*
- *custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto*
- *consegnare i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili,..) obsoleti all'amministratore di sistema per l'opportuna distruzione onde evitare che il loro contenuto possa essere successivamente alla cancellazione, recuperato.*

L'utente è responsabile del PC portatile assegnatogli e deve:

- *applicare al PC portatile le regole di utilizzo previste per i PC connessi in rete*
- *custodirlo con diligenza e in luogo protetto durante gli spostamenti*
- *rimuovere gli eventuali file elaborati sullo stesso prima della sua riconsegna*

Utilizzo delle stampanti e dei materiali d'uso

Stampanti e materiali di consumo in genere (carta, inchiostro, toner, floppy disk, supporti digitali come CD e DVD) possono essere usati esclusivamente per compiti di natura strettamente istituzionale, evitando in ogni modo sprechi e utilizzi eccessivi.

Gli utenti devono effettuare la stampa dei dati solo se strettamente necessaria e ritirare prontamente dai vassoi delle stampanti comuni i fogli per impedire a persone non autorizzate di accedere alle stampe di documenti riservati

Distruggere personalmente e sistematicamente le stampe che non servono più.

È fatto divieto assoluto di effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi, salvo:

- *diversa disposizione esplicita del titolare del trattamento, da concordarsi di volta in volta e comunque sempre preventivamente al trattamento*
- *informazione preventive degli interessati*
- *acquisizione del loro libero consenso, preventivo ed informato*

Il datore di lavoro, per esigenze organizzative, per garantire la sicurezza sul lavoro, per evitare reiterati comportamenti dolosi illeciti può avvalersi legittimante, nel rispetto dell'art. 4 commi 1 e 2 dello statuto dei lavoratori[1], di sistemi che consentano un controllo a distanza e determinato di dati personali riferibili a singoli utenti.

Il datore di lavoro non può in alcun caso utilizzare detti sistemi per ricostruire l'attività del lavoratore tramite:

- *memorizzazione sistematica delle pagine web visualizzate*
- *lettura e registrazione dei caratteri inseriti dai lavoratori tramite tastiera o dispositivi analoghi*
- *analisi occulta dei dispositivi per l'accesso a internet o alla posta elettronica messi a disposizione dei dipendenti*

Le attività sull'uso del servizio di accesso ad internet vengono automaticamente registrate attraverso il log di sistema ottenuti da un proxy server o da altro strumento di registrazione delle informazioni. Tali file possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazione della normativa vigente.

I dati contenuti nei log sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di verifica delle funzionalità dei sistemi di protezione e comunque non per più di due mesi. Dopo tale periodo il sistema cancella automaticamente tali tracciati.

La riservatezza delle informazioni registrate è soggetta a quanto dettato dal D. lgs. n.° 196/2003, il trattamento dei dati avviene esclusivamente per fini istituzionali, per attività di monitoraggio e controllo e in forma anonima in modo tale da precludere l'identificazione degli utenti o delle loro attività. Le registrazioni possono essere utilizzate per fornire informazioni esclusivamente su:

- *numero di utenti che visita ciascun sito o dominio, numero di pagine richieste e quantità dati scaricati*
- *numero di siti visitati da ciascun utente, quantità totale di dati scaricati, postazioni di lavoro utilizzate per la navigazione*

I dati personali contenuti nei log possono essere utilizzati tassativamente solo nelle seguenti ipotesi:

---

11. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione delle sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi. (2)
2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

- *per corrispondere ad eventuali richieste dell'autorità giudiziaria e della polizia postale*
- *quando si verifichi un evento dannoso o una situazione di pericolo che richiede un immediato intervento*
- *in caso di utilizzo anomalo degli strumenti, da parte degli utenti, reiterato nonostante l'esplicito invito ad attenersi alle istruzioni impartite.*

Qualora i controlli evidenzino un utilizzo anomalo degli strumenti informatici dell'istituto, il titolare del trattamento procede in forma graduata:

- *in via preliminare si eseguono controlli su dati aggregati, in forma anonima e si provvede ad un avviso generalizzato agli utenti*
- *se perdurano le anomalie si procede a controlli per tipologie di locali di utilizzo (uffici, aule,..) o tipologie di utenti (ata, docenti, studenti,..) e si procede con avvisi mirati alle categorie di utilizzatori*
- *ripetendosi l'anomalia, sarà lecito il controllo su base individuale e si procederà all'invio di avvisi individuali*
- *in caso di verificato e reiterato uso non conforme delle risorse informatiche il titolare del trattamento attiva il procedimento disciplinare*

I trattamenti in servizio proxy sono curati da personale tecnico incaricato del trattamento.

Il presente regolamento è messo a disposizione degli utenti, per la consultazione, sui mezzi di comunicazione interna utilizzati dall'istituto (circolare, sito) e quindi portato a conoscenza di ciascun dipendente.

L'utente qualora l'istituto decidesse di perseguire, per fini legati alla sicurezza dell'intero sistema informativo, il controllo della navigazione in internet, viene informato degli strumenti e del modo di trattamento effettuati prime che questo sia iniziato.

La contravvenzione alle regole contenute nel presente regolamento da parte di un utente:

- *può comportare l'immediata revoca delle autorizzazioni ad accedere alla rete informatica ed ai servizi/programmi autorizzati, fatte salve le sanzioni più gravi previste dalla enorme vigenti*
- *è perseguibile con provvedimenti disciplinari nelle forme e con le modalità previste dall'istituto per gli studenti, dai contratti di lavoro per i dipendenti e attraverso l'adozione degli atti di specifica competenza nel caso di personale non dipendente*
- *può portare alle azioni civili e penali consentite.*

L'utilizzo dei servizi di accesso ad internet cessa o viene sospesa d'ufficio quando:

- *non sussiste più la condizione di dipendente/studente o l'autorizzazione al loro uso*
- *vi è il sospetto di manomissione dell'hardware o del software*
- *in caso di diffusione o comunicazione a terzi da parte del dipendente di password, codici di accesso ecc,..*
- *in caso di accesso doloso a file o servizi non rientranti tra quelli autorizzati*
- *ogni qual volta sussistano ragionevoli evidenze di una violazione degli obblighi dell'utente*
- *che mette a rischio il sistema*

Il presente regolamento è soggetto a revisione ogni qual volta sia necessario un aggiornamento alla luce dell'esperienza, di nuove normative e dell'innovazione tecnologica.

Tutti gli utenti possono proporre quando ritenuto necessario, integrazioni al presente regolamento e le proposte saranno esaminate dal responsabile del trattamento in collaborazione con l'amministratore di sistema.

Il Dirigente Scolastico

[1]*Il documento è firmato digitalmente ai sensi del D.lgs. 82/2005 s.m.i. e norme collegate e sostituisce il documento cartaceo e la firma autografa.*