Ministero dell'Istruzione

ISTITUTO COMPRENSIVO SAPONARA

Via Firenze - Saponara (ME) - Tel. /Fax 090/333120
Via Antonello – Spadafora – Tel./Fax 090/9941778
Corso F. Saija, 86 – Rometta Marea – Tel./Fax 090/9961742
Cod. fiscale: 97062220831 - Cod. meccanografico: MEIC87400N
e-mail: **meic87400n@istruzione.it**- pec: **meic87400n@pec.istruzione.it**
sito web: **www.icsaponara.edu.it**
Codice univoco ufficio UF4TSQ
****

DISCIPLINARE INTERNO PER L'UTILIZZO DI POSTA ELETTRONICA, INTERNET E PDL

Rev 1.1 del 12/03/2020

INDICE

Indice **2**

1. INTRODUZIONE **3**

2. il regolamento europeo in materia di tutela del trattamento dei dati personAli **4**

2.1 principi generali 4

2.2 principi del codice 4

3 adozione di misure organizzative **4**

4 ADOZIONE DI MISURE DI TIPO TECNOLOGICO **5**

5 prescrizioni sull'uso della rete internet **5**

5.1 comportamenti e misure applicative rispetto la navigazione internet 5

6 prescrizioni sulla gestione della posta elettronica **5**

6.1 comportamenti e misure applicate rispetto all'utilizzo della posta elettronica 6

7 prescrizioni sulla gestione della POSTAZIONE DI LAVORO **7**

Linee guida per la prevenzione dei Virus **9**

Come si trasmette un virus: **9**

Come NON si trasmette un virus: **9**

Quando il rischio da virus si fa serio: **9**

Quali effetti ha un virus? **9**

Come prevenire i Virus **9**

Scelta delle Password **10**

Cosa NON fare **10**

Cosa fare **10**

8 Trattamento dei dati da postazioni remote ("SMART WORKING" o LAVORO AGILE) **10**

9 controlli e correttezza nel trattamento dei dati sui lavoratori **11**

9.1 disciplina intErna 11

9.2 apparecchiature preordinate al controllo a distanza 11

9.3 programmi che consentono controlli indiretti 12

9.4 gestione internet e posta elettronica 12

9.5 memorizzazione informazioni 12

9.6 informativa 13

1. INTRODUZIONE

Il presente documento viene redatto dall'Istituto in Intestazione, titolare delle operazioni di trattamento (di seguito indicato per brevità "Titolare"), in adempimento a quanto prescritto dal Garante per la protezione dei dati personali nel provvedimento a carattere generale del 01/03/2007 con il quale sono state prescritte ai datori di lavoro (pubblici e privati) alcune misure, necessarie o opportune, per confrontare il trattamento dei dati personali effettuato in Istituto alle disposizioni vigenti in materia, al fine di verificare il corretto utilizzo, nel rapporto di lavoro, della posta elettronica e della rete internet.

Per comprendere pienamente l'importanza di tale documento occorre muovere alcune premesse:

- compete al Titolare assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori difendendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;
- spetta al dator di lavoro adottare idonee misure di sicurezza per garantire la disponibilità e l'integrità dei sistemi informativi e dei dati, anche al fine di prevenire utilizzi indebiti che possono innescare meccanismi di responsabilità ex artt 24,25,28,82,83 del Regolamento Europeo 679/16 in materia di protezione dei dati personali.
- Emerge l'esigenza di tutelare i lavoratori interessati anche perché l'utilizzo dei mezzi Istituzionali, già ampiamente diffuso nel contesto lavorativo, è destinato a aumentare rapidamente anche in relazione alle attività svolte fuori dalla sede lavorativa;
- L'utilizzo di internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni. I server di posta elettronica sono parimenti suscettibili, anche attraverso la tenuta di log file di traffico e mail a l'archiviazione di messaggi, di controllo che possono giungere fino alla conoscenza, da parte del Titolare (titolare del trattamento) del contenuto della corrispondenza.
- Le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili.

2. IL REGOLAMENTO EUROPEO IN MATERIA DI TUTELA DEL TRATTAMENTO DEI DATI PERSONALI

2.1 PRINCIPI GENERALI

Nell'impartire le seguenti prescrizioni il Garante tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione, efficacia, liceità, trasparenza, correttezza, minimizzazione, esattezza integrità e riservatezza di cui all'art 5 del suddetto regolamento.

2.2 PRINCIPI DEL CODICE

I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi in osservanza ai principi cogenti di:

- Necessità e limitazione delle finalità, secondo il quale i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione dei dati personali e dei dati identificativi in relazione alle finalità perseguite; i trattamenti devono, inoltre essere effettuati per finalità determinate esplicite e legittime osservando il principio di pertinenza e non eccedenza (art 5 co 1 par b, c, d). Il Titolare deve trattare i dati nella misura meno invasiva possibile; le attività di monitoraggio devono essere svolte solo da soggetti preposti e devono essere mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati personali e, se pertinente, del principio di segretezza della corrispondenza (Parere n. 8/2001, cit., punti 5 e 12)
- Il principio di correttezza, secondo il qual le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art 5 co 1 par a). Le tecnologie dell'informazione permettono di svolgere trattamenti ulteriori ed aggiuntivi rispetto a quelli specificamente inerenti all'attività lavorativa. Questo può avvenire all'insaputa o senza la piena consapevolezza del lavoratore se si considera che le potenziali applicazioni delle misure di sicurezza (dettagliate nel paragrafo successivo), sono di regola, poco conosciute dagli interessati.

3 ADOZIONE DI MISURE ORGANIZZATIVE

In osservanza al provvedimento del Garante del 01/03/2007 l'Istituto ha provveduto ad adottare le misure organizzative previste e segnatamente:

- Ha valutato con attenzione l'impatto sui diritti dei lavoratori prima dell'installazione di apparecchiature suscettibili di consentire il controllo a distanza e dell'eventuale trattamento di dati.
- Ha previsto, per i lavoratori ai quali è stato accordato l'utilizzo degli strumenti di posta elettronica ed internet, un'adeguata pubblicazione della policy interna Istituzionale, istituendo anche uno specifico corso di formazione, rispetto al corretto uso dei mezzi e con riferimento agli eventuali controlli sulla modalità di utilizzo degli stessi strumenti.
- Il titolare del trattamento ha preventivamente individuato i lavoratori ai quali è accordato l'utilizzo della posta elettronica e l'accesso ad internet
- Il titolare del trattamento ha determinato quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di un impiego abusivo. Nello specifico:
    - ufficio di segreteria didattica;
    - ufficio di segreteria contabile;
    - ufficio di segreteria del personale;
    - ufficio di presidenza;

- ufficio di vice presidenza;
- laboratori didattici;

4 ADOZIONE DI MISURE DI TIPO TECNOLOGICO

In ottemperanza al provvedimento del garante del 01/03/2007 l'Istituto ha provveduto ad adottare le misure tecnologiche come di seguito prescritte:

- Il titolare del trattamento ha configurato i sistemi o l'utilizzo di filtri prevedendo determinate operazioni, reputate inconferenti con l'attività lavorativa
- Il titolare del trattamento raccomanda, ogni qualvolta sia possibile, il trattamento dei dati in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune integrazioni.
- Il titolare del trattamento prevede che la conservazione nel tempo dei dati sia strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

5 PRESCRIZIONI SULL'USO DELLA RETE INTERNET

La navigazione internet è consentita per attività e sviluppo di progetti strettamente ed inequivocabilmente connessi all'attività lavorativo svolta in relazione alla mansione affidata al dipendente.

5.1 COMPORTAMENTI E MISURE APPLICATIVE RISPETTO ALLA NAVIGAZIONE INTERNET

Il Titolare ha individuato i comportamenti non consentiti all'interno dell'Istituto e le misure applicate in riferimento alla navigazione in internet oppure alla tenuta di fale nella rete interna:

- Non è consentito l'accesso o la navigazione in internet se non a mezzo della rete Istituzionale e per fini esclusivamente lavorativi; è pertanto tassativamente vietato l'utilizzo di modem personali se non nei casi espressamente e formalmente autorizzati dall'Istituto nella qualità di titolare del trattamento.
- Non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on line e simile, salvo nei casi espressamente e formalmente autorizzati dall'Istituto nella qualità del titolare del trattamento;
- Non è permessa la partecipazione, per motivi non professionali, a forum o l'utilizzo di chat line, social networks, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi, salvo nei casi espressamente e formalmente autorizzati dall'Istituto nella qualità di Titolare del Trattamento; è comunque consentito nella fascia oraria dalle 13 alle 15
- I download consentiti sono: file allegati alle e mail in formato word, pdf e similari.

6 PRESCRIZIONI SULLA GESTIONE DELLA POSTA ELETTRONICA

Il Titolare consente l'utilizzo della posta elettronica anche per moderato uso personale.

- Il titolare del trattamento ha ritenuto necessario mettere a disposizione di ciascun lavoratore, apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate o fine rapporto di lavoro, messaggi di risposta che contengano le coordinate di altro soggetto o altre utili modalità o informazioni di contatto della struttura presso la quale opera il lavoratore assente.

- Il titolare del trattamento, in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa o fine rapporto lavorativo, si debba conoscere il contenuto dei messaggi di posta elettronica, ha nominato il responsabile del reparto nel quale in lavoratore è inserito a verificare il contenuto dei messaggi e ad inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.
- I messaggi di posta elettronica contengono un avvertimento rivolto ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando che le risposte ai messaggi potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla policy privacy.
- Il titolare del trattamento non concede la possibilità di un'eventuale attribuzione al lavoratore di un diverso indirizzo destinato ad uso privato.

6.1 COMPORTAMENTI E MISURE APPLICATE RISPETTO ALL'UTILIZZO DELLA POSTA ELETTRONICA

Il Titolare individua i comportamenti non consentiti e le misure applicative rispetto all'utilizzo di posta elettronica:

- Non è consentito utilizzare l'indirizzo di posta elettronica per inviare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria con riferimento al sesso, alla lingua, alla religione, alla razza, all'origine etnica, alle condizioni di salute, all'opinione politica e all'appartenenza sindacale.
- Non è consentito utilizzare l'indirizzo di posta elettronica per la partecipazione a dibattiti, forum o mailing list su internet per motivi non professionali; non è altresì consentito aderire o rispondere a messaggi che invitano a perpetrare documenti o contenuti verso ulteriori indirizzi e mail (es. catene di sant'Antonio).
- Non è consentiti effettuare nessun tipo di comunicazione finanziaria ivi comprese le operazioni di remote banking, acquisti on line e similari, salvo diversa ed esplicita autorizzazione del Titolare.
- Non è consentito simulare l'identità di un altro utente, ovvero utilizzare le credenziali di posta elettronica non proprie, per l'invio di messaggi.
- Non è consentito prendere visione delle e-mail altrui.
- Non è consentito aprire allegati di posta elettronica il cui contenuto è palesemente al di fuori dalle mansioni lavorative richieste
- Non è consentito al dipendente modificare, per nessun motivo, la configurazione hardware e software della sua macchina; né è consentita la possibilità di utilizzare sistemi client di posta elettronica non conformi a quelli accettati dall'Istituto;
- Non è consentito l'utilizzo di sistemi di crittografia o di qualsiasi altro programma di sicurezza non previsto esplicitamente dal servizio informatico Istituzionale;
- Non è consentita la trasmissione a mezzo posta elettronica di dati sensibili e/o commerciali di alcun genere se non nell'ambito della nomina di incaricato al trattamento dei dati ricevuta.

7 PRESCRIZIONI SULLA GESTIONE DELLA POSTAZIONE DI LAVORO

Istruzioni agli addetti al trattamento che trattano dati con strumenti elettronici corredate di Linee Guida per la Prevenzione dei Virus e per la scelta delle password

Nell'ambito informatico, il termine "sicurezza" si riferisce a tre aspetti distinti:

1. **Riservatezza**: Prevenzione dell'accesso non autorizzato alle informazioni
2. **Integrità:** Le informazioni non devono essere alterabili da incidenti o abusi
3. **Disponibilità**: Il sistema deve essere protetto da interruzioni impreviste

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi, misure soltanto tecniche, per quanto possono essere sofisticate, non saranno efficienti se non usate propriamente. In particolare, le precauzioni di tipo tecnologico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

- **Utilizzare le chiavi**: il primo livello dì protezione di qualunque sistema è quello fisico: è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario, non banale, per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio e riponete i documenti negli appositi contenitori alla fine di ogni giornata di lavoro.
- **Conservare i documenti in luoghi sicuri**: tutti i documenti cartacei devono essere posti in contenitori con etichette che devono riportare un identificativo ma mai con i nominativi di studenti, fornitori o contatti o qualsiasi altra informazione immediatamente riconducibile a persone fisiche. Tutti i contenitori con i documenti devono essere posti in scaffalature a giorno; se poste in luoghi controllati, o in armadi con serratura o ripostigli con porte con serratura se posti in luoghi non controllati o aperti al pubblico. I dati per cui viene richiesto il blocco o la cancellazione, che devono essere mantenuti per un obbligo di legge o a propria tutela in quanto relativi ad adempimenti contrattuali svolti, dovranno essere posti in armadi con serratura o ripostigli con porte con serratura. I dati sensibili o giudiziari dovranno sempre essere posti in armadi con serratura o ripostigli con porte con serratura e sono consegnati agli incaricati sotto la loro responsabilità e, al di fuori dell'orario di lavoro, solo previa registrazione. I dati estremamente riservati dovranno essere posti in armadi blindati, casseforti o luoghi sicuri (locali in muratura con porta blindata). Non lasciare documenti con dati personali sui tavoli, dopo averli utilizzati; riponeteli sempre nei loro contenitori.
- **Conservare i CD in un luogo sicuro**: per i CD, DVD, dischetti, pen-drive e per qualsiasi altro supporto removibile di dati, si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può essere anche dovuto ad, un furto) può passare più facilmente inosservato. Riponeteli quindi sotto chiave in armadi o archivi non appena avete finito di usarli.
- **Utilizzate le password**: vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:
    - la password di accesso al computer che impedisce l'utilizzo improprio della vostra postazione quando per un motivo qualsiasi non vi trovate in ufficio;
    - la password di accesso alla rete che impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'ufficio;
    - la password di programmi specifici che impedisce l'accesso ai documenti realizzati con quelle applicazioni;
    - la password del salvaschermo, infine, impedisce che una vostra assenza momentanea permetta persona non autorizzata di visualizzare il vostro lavoro.

- L'utilizzo di questi tipi fondamentali di password è obbligatorio. Imparatene l'utilizzo, e nel caso dobbiate comunicare, almeno temporaneamente, ai tecnici incaricati dell'assistenza, la vostra password registrate l'ora di comunicazione e di rinnovo della vostra password.
- **Attenzione alle stampe e ai fax di documenti riservati:** non lasciate accedere alle stampe o ai fax persone non autorizzate, se la stampante o il fax non si trovano sulla vostra scrivania recatevi quanto prima a ritirare le stampe. Posizionate le stampanti e i fax in luoghi controllati e non accessibili al pubblico ed a visitatori. Distruggete personalmente le stampe quando non servono più. È opportuno l'utilizzo di una macchina distruggi documenti, indispensabile nel caso di documenti sensibili o giudiziari.
- **Non utilizzate le mail per dati riservati**: non inviate MAI dati riservati via email come numeri di carta di credito, password, numeri di conti bancari.
- **Prestate attenzione all'utilizzo dei computer portatili**: i computer portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido e utilizzate una procedura di backup periodico. Se durante la giornata vi spostate molto dalla vostra postazione o addirittura la notte lasciate il vostro portatile in ufficio, riponetelo in armadi chiusi a chiave.
- **Non fatevi spiare quando state digitando la password**: anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete una buona capacità di digitazione.
- **Custodite la password in un luogo sicuro**: scrivete la vostra password, chiudetela in busta chiusa e consegnatela all'incaricato addetto alla sua custodia che provvederà a firmarla nei lembi di chiusura. Fate ben attenzione a non riscrivere la vostra password, l'unico affidabile dispositivo di registrazione è la vostra memoria.
- **Non fate usare il vostro computer a personale esterno a meno di non essere sicuri della loro identità e delle loro autorizzazioni**: personale esterno può avere bisogno di installare del nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro computer.
- **Non utilizzate connessioni ad internet "hotspot"**: l'utilizzo di modem su postazioni di lavoro collegati alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer ma a tutti i dati dell'organizzazione. Per l'utilizzo consultatevi con il responsabile del trattamento dati.
- **Non installate programmi non autorizzati:** solo i programmi acquistati dalla vostra organizzazione con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici consultatevi con il responsabile del trattamento dati.
- **Adottate con cura le linee guida per la prevenzione di virus:** la prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di tutti i dati.
- **Controllate la politica locale relativa ai backup:** i vostri dati potrebbero essere gestiti su un server, oppure essere gestiti in locale e trasferiti in un server solo al momento del backup. Chiedete al responsabile del trattamento dati quali sono le operazioni di backup che dovete eseguire, con quali modalità e con quali tempi. Il responsabile del trattamento curerà con estrema cura ed attenzione i backup periodici di tutti i dati.
- **Utilizzate gruppi di continuità:** verificare lo stato di funzionamento e l'effettiva attivazione di gruppi di continuità, se presenti.

- **Segnalate le anomalie:** segnalate sempre, al più presto, al responsabile del trattamento dati, qualsiasi tipo di anomalia si verifichi, sia nelle funzionalità del computer in cui operate, sia sulla rete di computer su cui operate, sia su qualsiasi altra applicazione che state utilizzando. Segnalare in tempo le anomalie e circostanziare gli eventi è fondamentale per prevenire problemi ben più consistenti.

Linee guida per la prevenzione dei Virus

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

Come si trasmette un virus:

- attraverso programmi provenienti da fonti non ufficiali;
- attraverso le macro di alcuni programmi;
- attraverso le email ricevute;
- attraverso il download da Internet.

Come NON si trasmette un virus:

- attraverso file di dati non in grado di contenere macro (file di testo, pdf, jpeg, ecc);
- attraverso email non contenenti allegati.

Quando il rischio da virus si fa serio:

- quando si installano programmi scaricati da internet;
- quando si copiano dati da supporti esterni;
- quando si scaricano documenti e allegati da messaggi di posta elettronica provenienti da mittenti sconosciuti;

Quali effetti ha un virus?

- Messaggi pubblicitari invadenti e persistenti, anche chiudendo i programmi o riavviando il computer;
- Nel menù appaiono funzioni extra non richieste;
- File e documenti risultano di colpo inaccessibili o introvabili;
- Le funzionalità dei computer rallentano repentinamente;
- Compaiono messaggi in lingue straniere, contenenti richieste in denaro.

Come prevenire i Virus

- **Usate soltanto programmi provenienti da fonti fidate**: copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzare programmi non autorizzati dal responsabile del trattamento dei dati.
- **Assicuratevi di non far partire accidentalmente il vostro computer da dischetto, CD o DVD**: infatti se il dischetto fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri file.
- **Assicuratevi che il vostro software antivirus sia aggiornato**: la tempestività nell'azione di bonifica è essenziale per limitare danni che un virus può causare; inoltre è vitale che il programma antivirus sia aggiornato periodicamente (non oltre sei mesi).
- **Assicuratevi che sul vostro computer sia attivato il Firewall**: verificate dalle preferenze del vostro computer o chiedete al responsabile del trattamento dati, che sul vostro computer sia attivato il Firewall e solo i privilegi di rete minimi necessari alle vostre esigenze d'accesso ai dati, oltretutto se sul vostro computer non vi collegate ad Internet o non inviate fax staccate il cavo telefonico per evitare possibili accessi
- **Non diffondete messaggi di provenienza dubbia:** se ricevete messaggi che avvisano di un nuovo virus pericolosissimo e che fanno riferimento ad una notizia proveniente dalla "Microsoft", ignoratelo, le email di questo tipo sono dette con terminologia anglosassone “hoax” (termine spesso tradotto in italiano con "bufala")

- **Non partecipate a "catene di S. Antonio" e simili**: analogamente, tutti i messaggi che vi invitano a "diffondete la notizia quanto più possibile" sono “hoax”. Anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna; sono tutti “hoax” aventi spesso scopi molto simili a quelli dei virus, per ciò utilizzare indebitamente le risorse informatiche.
- **Non aprite allegati alle email inviate da sconosciuti**: non aprite allegati alle email con file di tipo exe, zip, sit, scr, doc, xls contenenti macro e qualsiasi altro formato a voi sconosciuto se non siete certi della provenienza. Potete aprire solamente allegati di tipo pdf, jpg e file di testo che non contengono macro.

Scelta delle Password

Il più semplice metodo per l'accesso illecito ad un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso non protetto da password "poco sicura". La scelta di password "sicure" è, quindi, parte essenziale della sicurezza informatica

Cosa NON fare

- **NON dite a nessuno la vostra password.** Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le Vostre risorse o possa farlo a Vostro nome.
- **NON scrivete la password da nessuna parte** che possa essere letta facilmente, soprattutto vicino al computer (es. su Post-it).
- **NON scegliete password che si possano trovare su un dizionario.** Su alcuni sistemi è possibile provare tutte le password contenute in un dizionario per vedere quale sia quella giusta.
- **NON crediate che usare parole straniere renderà più difficile il lavorò di scoperta**, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
- **NON usate il Vostro nome utente.** È la password più semplice da indovinare.
- **NON usate password che possono in qualche modo essere legate a Voi** come, ad esempio, il Vostro nome, quello di vostra moglie/marito, dei figli, del cane, date di nascita, numeri di, telefono, ecc.
- **NON impostate la funzionalità “memorizza password” nel browser internet.** Anche se è una funzionalità comoda, riduce la sicurezza delle vostre password.

Cosa fare

- Cambiare la password a intervalli regolari. La normativa sulla privacy prevede che se sono trattati dati sensibili o giudiziari la password deve essere cambiata ogni tre mesi altrimenti ogni sei mesi. La password deve essere lunga almeno otto caratteri, meglio se con un misto di lettere, numeri e caratteri speciali (es. $,!,#).
- Utilizzate password distinte per l'accesso avari sistemi.
- Le migliori password sono quelle facili da ricordare ma, allo stesso tempo, difficili da indovinare, come quelle che si possono ottenere comprimendo frasi lunghe (es. “Trentatretrentini$33”)

8 TRATTAMENTO DEI DATI DA POSTAZIONI REMOTE (“SMART WORKING” O LAVORO AGILE)

Nel caso in cui il trattamento dei dati sia svolto lontano dagli uffici amministrativi attraverso dispositivi come smartphone, tablet e laptop personali, il lavoratore è l’unico responsabile della sicurezza e dell’integrità del dispositivo. A tal proposito, è vietato accedere attraverso smart working da dispositivi personali che:

- abbiano subito violazioni, abusi o manomissioni (es. hacking);
- non siano dotati di un sistema antivirus aggiornato e funzionante;

- non abbiano ricevuto tutti gli aggiornamenti di sicurezza del produttore;
- non abbiano impostata una password di accesso.

Inoltre, il lavoratore è tenuto a non memorizzare alcun file, elenco o informazione all'interno del dispositivo personale, ma limitarsi soltanto all'utilizzo via web delle piattaforme e delle applicazioni autorizzate e comunicate dal Dirigente Scolastico.

Valgono, in tutti i casi, le disposizioni come da punti 5, 6 e 7 del presente disciplinare.

9 CONTROLLI E CORRETTEZZA NEL TRATTAMENTO DEI DATI SUI LAVORATORI

9.1 DISCIPLINA INTERNA

In base al già richiamato principio di correttezza di cui all'art 5 co. 1 lett a) del reg ue 679/16, l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevedono anche la normativa di settore all'art 4 co. 2 dello statuto dei lavoratori, ed il par. 3 del d. lgs 626/1994 e successive integrazioni in materia di uso di attrezzature munite di videoterminali che esclude la possibilità del controllo informatico all'insaputa dei lavoratori.
Grava quindi sul Titolare l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette ed in quali misure e con quali modalità vengano effettuati controlli.
Ciò tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali.
Nella sua qualità di Titolare e di titolare del trattamento si riserva la facoltà di effettuare controlli di conformità alla legge, anche saltuari o occasionali, sia per eseguire verifiche sulla funzionalità e sicurezza del sistema sia per verificare il corretto utilizzo da parte dei propri dipendenti tanto della rete internet che della posta elettronica.
I predetti controlli si svolgeranno in forma graduata:
in via preliminare l'Istituto provvederà ad eseguire dei controlli su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree ed ad un controllo anonimo che si concluderà con un avviso generalizzato relativo al rilevato utilizzo anomalo degli strumenti Istituzionali.
In assenza di anomalie non si effettueranno controlli individuali.
In presenza di anomalie si procedura a controlli su base individuale o delle postazioni di lavoro.
In caso di abusi singoli e reiterati si procederà all'invio di avvisi individuali e si eseguiranno controlli nominativi o su singoli dispositivi e/o postazioni di lavoro.
In caso di riscontrato e reiterato uso non conforme alle risorse informatiche, L'amministratore di sistema o la figura equipollente, che effettua i controlli, segnalerà il comportamento al titolare del trattamento il quale attiverà il procedimento disciplinare nelle forme e nelle modalità previste dal c.c.n.l.

9.2 APPARECCHIATURE PREORDINATE AL CONTROLLO A DISTANZA

Con riguardo al principio secondo il quale occorre perseguire finalità determinate, esplicite e legittime di cui all'art 5 co. 1 b) del Reg. UE 679/16, il Titolare può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (art.t 2086, 2087, 2104 c.c.).
Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (art 4 co. 1 L. n. 300/70) tra le quali sono certamente

ricomprese le strumentazioni hardware e software mirate al controllo dell'utente di un sistema di comunicazione elettronica.
Il trattamento dei dati che ne consegue è illecito, a prescindere dall'illiceità dell'installazione stessa. Ciò anche quando i singoli lavoratori ne siano consapevoli.
In particolare non può ritenersi consentito il trattamento effettuato mediante sistemi hardware e software preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire l'attività dei lavoratori.

9.3 PROGRAMMI CHE CONSENTONO CONTROLLI INDIRETTI

Il Titolare, utilizzando sistemi informativi per esigenze produttive o organizzative, o comunque quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello statuto dei lavoratori (art 4 comma 2), di sistemi che consentono indirettamente un controllo a distanza con correlato trattamento di dati personali riferiti o riferibili ai lavoratori.
Il trattamento dei dati che ne consegue può considerarsi lecito. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione da parte dei lavoratori o dei sindacati in relazione all'introduzione e alla modifica di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.

9.4 GESTIONE INTERNET E POSTA ELETTRONICA

Nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, come pure dei soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata. L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza. Nel caos in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il Titolare può adottare eventuali misure che consentano la verifica di comportamenti anomali.
Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti Istituzionali e con l'invito ad attenersi scrupolosamente ai compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia.
In assenza di successive anomalie no è di regola giustificato effettuare controlli su base individuale.
Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

9.5 MEMORIZZAZIONE INFORMAZIONI

I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad internet e al traffico telematico, la quale conservazione non sia necessaria.
Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione a:

1) Esigenze tecniche o di sicurezza eccezionali;
2) Indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
3) Obbligo di custodire o consegnare dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Sono temporaneamente memorizzate, da parte degli incaricati amministratori di sistema, le seguenti informazioni:

- La data e l'ora del log in e del log off del servizio di accesso ad internet, unitamente all'indirizzo IP assegnato dal fornitore di accesso ad internet come anche l'identificativo dell'utente registrato.
- La data e l'ora del log in e log off del servizio di posta elettronica

- Le informazioni relative all'utilizzo della posta elettronica e all'accesso internet sono tracciate e conservate per finalità organizzative di sicurezza e di controllo da parte dell'Istituto per un periodo minimo di una settimana e massimo di due mesi.

9.6 INFORMATIVA

All'onere in capo al Titolare di predisporre e pubblicizzare una policy interna rispetto al corretto uso dei mezzi e agli eventuali controlli sullo stesso, si affianca il dovere di informare comunque gli interessati ai sensi degli artt. 12, 13, 14 del Reg. UE 679/16.

Nello specifico l'informativa potrà essere distribuita a tutti i lavoratori tramite:

- consegna a mano con relativa firma
- intranet Istituzionale
- sito web istituzionale

IL DIRIGENTE SCOLASTICO
Emilia Arena
Documento informatico firmato digitalmente
ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate,
il quale sostituisce il documento cartaceo e la firma autografa