Raccomandazioni generali per la sicurezza e la protezione dei dati personali

1. Informazioni Generali

1.1. Definizioni

Autorizzazione: il provvedimento adottato dal Garante con cui il titolare del trattamento (ente pubblico, impresa, libero professionista) viene autorizzato a trattare determinati dati "sensibili" o giudiziari, ovvero a trasferire dati personali all'estero.

Comunicazione: far conoscere dati personali a uno o più soggetti determinati (che non siano l'interessato, il Responsabile/Autorizzato/Incaricato/Designato, in qualunque forma, anche attraverso la loro messa a disposizione o consultazione (vedi anche diffusione)

Consenso: la libera manifestazione di volontà dell'interessato con cui questi accetta espressamente un determinato trattamento dei suoi dati personali, del quale è stato preventivamente informato da chi ha un potere decisionale sul trattamento (vedi titolare).

D.Lgs. 196/2003: Decreto Legislativo 196 del 30 giugno 2003 e sue successive modifiche ed integrazioni.

Dato personale: qualsiasi informazione che riguardi persone fisiche identificate o che possono essere identificate anche attraverso altre informazioni, ad esempio, attraverso un numero o un codice identificativo. Sono, ad esempio, dati personali: il nome e cognome o denominazione; l'indirizzo, il codice fiscale; ma anche un'immagine, la registrazione della voce di una persona, la sua impronta digitale, i dati sanitari, i dati bancari, ecc.

Dato particolare: un dato personale che, per la sua natura, richiede particolari cautele: sono dati particolari (sensibili) quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose o di altra natura, le opinioni politiche, l'adesione a partiti, sindacati o associazioni, lo stato di salute e la vita sessuale delle persone.

Dato giudiziario: i dati personali che rivelano l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (quali, ad es., i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione). Rientrano in questa categoria anche la qualità di imputato o di indagato.

Diffusione: divulgare dati personali al pubblico o, comunque, ad un numero indeterminato di soggetti (ad esempio, è diffusione la pubblicazione di dati personali su un quotidiano o su una pagina web).

Dipendente: personale dell'Istituzione Scolastica assunto con qualsiasi tipo di forma contrattuale.

GDPR General Data Protection Regulation - Regolamento Generale sulla Protezione dei Dati - UE 2016/679: è un Regolamento con il quale la Commissione europea intende rafforzare e rendere più omogenea la protezione dei dati personali di cittadini dell'Unione Europea e dei residenti nell'Unione Europea, sia all'interno che all'esterno dei confini dell'Unione europea (UE). Il testo, pubblicato su Gazzetta Ufficiale Europea il 4 maggio 2016 ha efficacia dal 25 maggio 2018.

Incaricato: ogni dipendente, come sopra identificato, ed ogni consulente esterno che, nell'ambito dell'attività assegnatagli, tratta dati (nell'accezione del capitolo seguente) riferiti all'Istituzione Scolastica. Il regolamento europeo non prevede espressamente la figura dell'incaricato, ma non ne esclude la nomina, facendo riferimento a persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile (art. 4). In sede europea, alla nostra DPA è stato concesso di poter utilizzare ancora i termini titolare, responsabile e incaricato; traducendo così, nella versione italiana del GDPR, la figura del "controller" (Art. 4.7) con "titolare del trattamento"; "processor" (Art. 4.8) con "responsabile del trattamento"; "third party" (Art. 4.10) con "terzo", e di poter continuare ad utilizzare il termine "incaricato" per qualificare "le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile". Alla luce di ciò, si può identificare la figura di Incaricato in quella di Responsabile.

Informativa: le informazioni che il titolare del trattamento deve fornire ad ogni interessato, verbalmente o per iscritto quando i dati sono raccolti presso l'interessato stesso, oppure presso terzi. L'informativa deve precisare sinteticamente e in modo colloquiale quali sono gli scopi e le modalità del trattamento; se l'interessato è obbligato o no a fornire i dati; quali sono le conseguenze se i dati non vengono forniti; a chi possono essere comunicati o diffusi i dati; quali sono i diritti riconosciuti all'interessato; chi sono il titolare e l'eventuale responsabile del trattamento e dove sono raggiungibili (indirizzo, telefono, fax, ecc.).
Misure di sicurezza: sono tutti gli accorgimenti tecnici ed organizzativi, i dispositivi elettronici o i programmi informatici utilizzati per garantire che i dati non vadano distrutti o persi anche in modo accidentale, che solo le persone autorizzate possano avere accesso ai dati e che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti.

NDA: non-disclosure agreement, ovvero accordo di non divulgazione, è un negozio giuridico di natura sinallagmatica che designa informazioni confidenziali e con il quale le parti si impegnano a mantenerle segrete, pena la violazione dell'accordo stesso e il decorso di specifiche clausole penali in esso contenute.

Responsabile (del trattamento): la persona, la società, l'ente, l'associazione o l'organismo cui il titolare affida, anche all'esterno, per la particolare esperienza o capacità, compiti di gestione e controllo del trattamento dei dati.

Titolare del trattamento: la persona fisica, l'impresa, l'ente, l'associazione, ecc. cui fa capo effettivamente il trattamento di dati personali e spetta assumere le decisioni fondamentali sugli scopi e sulle modalità del trattamento medesimo (comprese le misure di sicurezza).
Nei casi in cui il trattamento sia svolto da una società o da una pubblica amministrazione per titolare va intesa l'entità nel suo complesso e non l'individuo o l'organo che l'amministra o la rappresenta (presidente, amministratore delegato, sindaco, ministro, direttore generale, ecc.).

Trattamento (di dati personali): un'operazione o un complesso di operazioni che hanno per oggetto dati personali.

1.2. Premessa

L'ambito lavorativo porta la nostra organizzazione scolastica a gestire una serie di "informazioni", proprie e di terzi, per poter erogare i servizi che le vengono istituzionalmente richiesti.
Tali informazioni possono essere considerate, ai sensi della normativa vigente, "dati personali" quando sono riferite a persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è necessario che l'Istituzione Scolastica adotti una serie di misure di sicurezza idonee alla protezione dei dati per come previsto dall'art. 32 del REG UE 679/2016.
Altre informazioni, pur non essendo "dati personali" ai sensi di legge, sono in tutto e per tutto "informazioni riservate", ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali l'Istituzione Scolastica è chiamata a garantire la riservatezza, o per NDA, o per una più ampia tutela del patrimonio dell'Istituzione Scolastica.
Ai fini di questo disciplinare si specifica, pertanto, che con il termine "dati" deve intendersi l'insieme più ampio di informazioni di cui un dipendente o un collaboratore può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i "dati personali" intesi a norma di legge.
Inoltre, nell'ambito della sua attività, L'Istituzione Scolastica tratta "dati cartacei", ovvero informazioni su supporto cartaceo, e "dati digitali", ovvero informazioni che vengono memorizzate o semplicemente transitano attraverso apparecchiature digitali.
In linea generale, ogni dato, nell'accezione più ampia sopra descritta, di cui l'incaricato viene a conoscenza, nell'ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con l'Istituzione Scolastica stessa o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita delL'Istituzione Scolastica.
Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta.

La progressiva diffusione delle nuove tecnologie informatiche ed, in particolare, l'accesso alla rete internet dal computer della scuola, espone l'Istituzione Scolastica a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine dell'Istituzione Scolastica stessa.
Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, tra i quali rientrano l'utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, L'Istituzione Scolastica ha adottato il presente Disciplinare Interno, diretto ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature scolastiche.
Il presente Disciplinare Interno si applica ai Responsabili e Incaricati/Designati/Autorizzati che si trovino ad operare con dati dell'Istituzione Scolastica.
Una gestione dei dati cartacei, un uso dei COMPUTER e di altre attrezzature elettroniche (di seguito DISPOSITIVI), nonché dei servizi internet e della posta elettronica difforme dalle regole contenute nel presente Disciplinare potrebbe esporre l'Istituzione Scolastica ad un maggiore rischio di accessi non autorizzati ai dati e/o al sistema informatico scolastica, furti o divulgazioni di informazioni riservate nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell'intero sistema informatico.
Le informazioni contenute nel presente Disciplinare costituiscono, parte integrante delle nomine conferite

1.3. Esclusione all'uso degli strumenti informatici

All'inizio del rapporto lavorativo o di consulenza, l'Istituzione Scolastica valuta la presenza dei presupposti per l'autorizzazione all'uso dei vari dispositivi scolastici, di internet e della posta elettronica da parte degli incaricati.
Successivamente, e periodicamente, l'Istituzione Scolastica valuta la permanenza dei presupposti per l'utilizzo dei dispositivi scolastici, di internet e della posta elettronica.
È fatto esplicito divieto ai soggetti non autorizzati di accedere agli strumenti informatici scolastici. I casi di esclusione possono riguardare:

1. L'utilizzo del COMPUTER o di altri DISPOSITIVI.
2. L'utilizzo della posta elettronica.
3. L'accesso a internet.

Le eventuali esclusioni sono strettamente connesse al principio della natura scolastica e lavorativa degli strumenti informatici, nonché al principio di necessità di cui al Codice Privacy e GDPR. Più specificatamente, hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo i responsabili che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno.
I casi in cui le esclusioni dovranno risultare operative in forza di tali motivazioni verranno comunicati individualmente e potranno riguardare sia tutti i casi sopra descritti, sia solo uno o due degli stessi.
Si informa che tali esclusioni sono divenute necessarie alla luce del Provvedimento del Garante 1° marzo 2007, che indica di ridurre a titolo cautelativo e preventivo l'utilizzo degli strumenti informatici in considerazione dei pericoli e delle minacce indicate in questo documento.

1.4. Titolarità dei dispositivi e dei dati

L'Istituzione Scolastica è esclusiva titolare e proprietaria dei dispositivi messi a disposizione dei responsabili, ai soli fini dell'attività lavorativa.
L'Istituzione Scolastica è l'unico esclusivo titolare e proprietario di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri dispositivi digitali o archiviati in modo cartaceo nei propri locali. Il Responsabile/Autorizzato/Incaricato/Designato non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei dispositivi scolastici (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i file di filmati o altre tipologie di file) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da lui copiati, comunicati o diffusi senza l'autorizzazione dell'Istituzione Scolastica.

1.5. Finalità nell'utilizzo dei dispositivi

I dispositivi assegnati sono uno strumento lavorativo nelle disponibilità dell'Incaricato/ Responsabile/Autorizzati/Designato esclusivamente per un fine di carattere lavorativo. I dispositivi, quindi, non devono essere utilizzati per finalità private e diverse da quelle istituzionali, se non eccezionalmente e nei limiti evidenziati dal presente Disciplinare.
Qualsiasi eventuale tolleranza da parte di questo Istituto, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Disciplinare.

1.6. Restituzione dei dispositivi

A seguito di una cessazione del rapporto lavorativo o di consulenza del Responsabile o Incaricato/Designato/Autorizzato con l'Istituzione Scolastica o, comunque, al venir meno, ad insindacabile giudizio dell'Istituzione Scolastica, della permanenza dei presupposti per l'utilizzo dei dispositivi scolastici, i responsabili/incaricati/autorizzati/designati hanno i seguenti obblighi:

1. Procedere immediatamente alla restituzione dei dispositivi in uso.
2. Divieto assoluto di formattare o alterare o manomettere o distruggere i dispositivi assegnati o rendere inintelligibili i dati in essi contenuti, tramite qualsiasi processo.

1.7. Restituzione dei dati cartacei

A seguito di una cessazione del rapporto lavorativo o di consulenza con l'Istituzione Scolastica o, comunque, al venir meno, ad insindacabile giudizio dell'Istituzione Scolastica, della permanenza dei presupposti per l'utilizzo di dati cartacei scolastici, gli autorizzati/incaricati/responsabili/designati hanno i seguenti obblighi:

1. Procedere immediatamente alla restituzione dei dati cartacei in loro possesso.
2. Divieto assoluto di alterare o manomettere o distruggere i dati cartacei assegnati o renderli inintelligibili, tramite qualsiasi processo, ai sensi del GDPR.

2. ANTIVIRUS

2.1 I virus (o, per essere precisi, il malware, il software malevolo) possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, condivisione di file, chat, o altro vettore.
L'Istituzione Scolastica impone su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente con frequenza almeno quotidiana.
Il Responsabile/Autorizzato/Incaricato/Designato, da parte sua, deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer e, in particolare, deve rispettare le regole seguenti:

1. Comunicare all'Istituzione Scolastica ogni anomalia o malfunzionamento del sistema antivirus.
2. Comunicare all'Istituzione Scolastica eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, al responsabile:

1. È vietato accedere alla rete scolastica senza servizio antivirus attivo e aggiornato sulla propria postazione.
2. È vietato ostacolare l'azione dell'antivirus.
3. È vietato disattivare l'antivirus senza l'autorizzazione espressa dell'Istituzione Scolastica, anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer.
4. È vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani. Contattare i sistemi informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

3. Internet è uno strumento di lavoro

3.1 La connessione alla rete internet dal dispositivo avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa. L'utilizzo per scopi personali è permesso con moderazione e con gli accorgimenti di cui al presente documento.
In particolare, si vieta l'utilizzo dei social network, se non espressamente autorizzati.

3.2. Misure preventive per ridurre navigazioni illecite

L'Istituzione Scolastica potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list.

3.3. Divieti Espressi concernenti Internet

– È vietata la navigazione nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute del Responsabile poiché potenzialmente idonea a rivelare dati sensibili ai sensi del Codice Privacy.
– È fatto divieto di accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
– È vietato al Responsabile o Incaricato/Designato/Autorizzato lo scarico (download) di software (anche gratuito) prelevato da siti Internet senza autorizzazione;
– È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dal Titolare e con il rispetto delle normali procedure di acquisto.
– È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
– È vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il logo o la denominazione dell'Istituzione Scolastica, salvo specifica autorizzazione dell'Istituto stesso.
– È vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
– È vietato al Responsabile o Incaricato/Designato/Autorizzato di promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica scolastica.
– È vietato accedere dall'esterno alla rete interna dell'Istituzione Scolastica, salvo con le specifiche procedure previste dall'Istituzione Scolastica stesso.
– È vietato, infine, creare siti web personali sui sistemi dell'Istituzione Scolastica, nonché acquistare beni o servizi su Internet, a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.
Ogni eventuale navigazione di questo tipo, comportando un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati personali e sensibili, è posta sotto la personale responsabilità del Responsabile o Incaricato/Designato/Autorizzato inadempiente.

4. Divieti di Sabotaggio

È vietato accedere ad alcuni siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dall'Istituzione Scolastica per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.

5. Diritto d'autore

È vietato utilizzare l'accesso ad internet, in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n.

633 e successive modificazioni, D. Lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere,...) se non espressamente autorizzato dall'Istituzione Scolastica.

I. Precauzioni generali nella cura e nella gestione degli strumenti elettronici

Gli operatori ed incaricati che utilizzano computer e periferiche informatizzate in genere devono attenersi alle precauzioni indicate nei relativi manuali, messi a disposizione dai fabbricanti e reperibili presso l'incaricato delegato o presso il responsabile della infrastruttura informatica.

Tutti gli autorizzati devono riferirsi al Responsabile o suo delegato al fine di conoscere le principali precauzioni, relative all'utilizzo corrente, in grado di prevenire guasti alle apparecchiature, danneggiamento e perdite di dati, e possibile trasferimento illecito su sistemi informativi e supporti non controllati.

1. Cercare di allontanare intensi campi magnetici dai computer e dai supporti magnetici, come ad esempio nastri, dischetti e simili. Se nel sistema vengono utilizzati degli altoparlanti, fate attenzione a che il potente campo magnetico del magnete non provochi danni alle apparecchiature (attenti alle lampade da tavolo con trasformatore incorporato nel basamento).
2. Non toccare mai la superficie dei supporti magnetici o dei contatti placcati in oro, come quelli che si trovano sui connettori multipoli o sui circuiti stampati ad innesto. I grassi animali presenti sulla superficie delle dita possono contaminare queste superfici e creare contatti incerti e anomalie funzionali, anche a distanza di tempo.
3. Proteggere sempre i computer, gli apparati terminali ed i supporti di registrazione da condizioni climatiche sfavorevoli, come ad esempio estremi di temperatura ed umidità, vapori corrosivi, liquidi, fumi, polvere od altre sostanze contaminanti.

II. Istruzioni attinenti al trattamento con strumenti elettronici

1. Tenere sotto controllo l'accesso fisico al computer e consentire l'accesso agli ambienti ove si trovano i sistemi informativi o le periferiche solo alle persone autorizzate. In caso di dubbio, non esitate a chiedere ai visitatori non noti e non accompagnati le ragioni della loro permanenza nei siti protetti. In caso di dubbio, rivolgetevi all'incaricato delegato od al responsabile del trattamento, anche telefonicamente.
2. Orientare gli schermi dei computer in maniera che essi non possano essere osservati da persone non autorizzate, ad esempio guardando attraverso le pareti vetrate di un corridoio, o finestre o porte aperte.
3. Non consentire l'accesso logico al computer a persone non autorizzate. In particolare:

- ricordarsi di effettuare il logoff della connessione con host o in rete locale, quando la sessione al terminale è finita o state abbandonando il vostro posto lavoro
- ricordarsi che archivi di dati possono rimanere memorizzati in memorie buffer di stampanti, di fax computerizzati ed altri terminali informatici (es. mezzi di scansione di rete). Accertarsi che tali memorie buffer siano sempre scaricate, al termine dell'utilizzo
- ricordarsi di spegnere il computer quando non lo state utilizzando
- mettere in sicurezza le aree operative non presidiate, ad esempio chiudendo a chiave la porta.

4. Identificare il livello di riservatezza di dati archiviati od elaborati nel computer ed adottate le appropriate misure sicurezza, secondo le specifiche istruzioni che vi sono state impartite.
5. Per sistemi informativi che usano sistemi di controllo logico dell'accesso basati su login, ID e parola chiave, accertarsi che gli identificativi logici personali usati siano conformi ai requisiti dello specifico sistema di controllo utilizzato. Vi ricordiamo che le parole chiave sono un sistema di protezione dell'accesso di largo uso, ma possono essere facilmente neutralizzate. Alcuni programmi automatici di penetrazione dei sistemi informativi possono rapidamente identificare parole comuni, nomi o combinazioni di caratteri, che vengono frequentemente utilizzati come parola chiave. È comportamento diligente la scelta di elementi identificativi non usuali e ragionevolmente complessi.
   - Se il sistema utilizza parola chiave di default, esse debbono esser cambiate subito. Non consentire che i controlli di sicurezza siano governati da parola chiave fornite dal fabbricante o dall'installatore;
   - Conservare in condizioni riservate il vostro codice identificativo personale. Divulgatelo solamente per comprovate ragioni, in condizioni strettamente controllate;
   - Non condividere con alcuno la vostra parola chiave e, se viene a conoscenza di terzi, cambiatela subito. La password, una volta impostata, va poi modificata periodicamente dall'utente titolare della postazione che è l'unico ad averne uso esclusivo.
   - Come regola generale, non scrivere le parole chiave. Se è necessario scriverla, conservate il documento in modo assolutamente sicuro, meglio se in forma camuffata;
   - Cambiare la parola chiave almeno ogni 180 giorni (in caso di trattamento di dati personali), e 90 (in caso di trattamento di dati personali sensibili), ed ogni volta che avete il sospetto che essa, per un motivo qualsiasi, sia venuta a conoscenza di terzi (ad esempio, per osservazione indiscreta);
   - Non inserire la parola chiave in programmi ed altri file, dove esse possono essere rintracciate;

II.1 La scelta e l'uso delle parole chiave

Nella maggior parte dei sistemi informativi, sono attivi dei sistemi di controllo dell'accesso logico, basati sull'utilizzo di parole d'ordine o parola chiave.

È dovere dell'operatore utilizzare con diligenza queste parole chiave, cambiandole spesso e non rivelandole ad alcuno.
Inoltre, la selezione della parola chiave, che è affidata all'incaricato, dovrebbe essere governata da criteri di casualità, evitando nel modo più assoluto di scegliere lettere tutte eguali, lettere o numeri comunque collegati alla persona, come date di nascita, nomi personali di familiari e simili. Ecco di seguito qualche altro prezioso consiglio su questo critico tema.

Cosa non fare

- Non usare il nome di login (o codice di identificazione personale) in qualsiasi forma (come è, invertito, in maiuscole, duplicato, ecc.)
- Non scegliere il nome o cognome, comunque modificato
- Non scegliere il nome del partner o dei figli
- Non usare informazioni su di voi, che possono essere facilmente recuperate, come la targa dell'autovettura, il numero di telefono, il codice fiscale, la marca della vostra autovettura, il nome della via dove abitate, ecc.
- Non scegliere parola chiave di meno di 8 caratteri alfanumerici
- Non scegliere una parola di senso compiuto in lingua italiana od una lingua straniera assai diffusa, come l'inglese
- Non usare caratteri sequenziali ripetuti (ad esempio 1111, aaaa, ecc.)
- Non usare cifre tutte a salire o scendere

Cosa fare

- Scegliere una parola chiave con caratteri minuscoli e maiuscoli
- Scegliere una parola chiave con segni di interpunzione
- Scegliere una parola chiave facile da ricordare, per non doverla trascrivere
- Scegliere una parola chiave facile da digitare, senza bisogno di scrutare la tastiera, per rendere difficile
- l'osservazione indiscreta
- Scegliere un verso di una canzone che ben conoscete e ricavate la parola chiave dalle iniziali delle prime parole o simili combinazioni
- Alternare consonanti e vocali, per creare parola chiave pronunciabili e quindi più facili da ricordare
- Scegliere due parole brevi e concatenarle con segni di interpunzione
- Cambiare spesso la parola chiave, massimo ogni 6 mesi in caso di sistemi informatici contenenti dati sensibili
- Usate la tastiera del cellulare per creare una connessione irreversibile tra caratteri alfabetici e numeri

Altre raccomandazioni

1. Proteggere dalla perdita o sottrazione od osservazione surrettizia qualsiasi dispositivo venga utilizzato per il controllo dell'accesso (chiavi, tessere magnetiche, codici di sicurezza, chiavi o dispositivi di cifratura)
1. Nota: la perdita o la sottrazione dei codici di cifratura richiede di solito la sostituzione di codici sia presso il mittente, sia presso il destinatario. Ciò può

produrre un intralcio alla regolarità del funzionamento dei sistemi di trasmissione. Prestare particolare attenzione alla protezione dei codici crittografici

2. Accertarsi che vengano eliminate o distrutte in modo sicuro le cartucce a nastro delle stampanti, le cartucce delle stampanti laser, i CD, i supporti magnetici, gli stampati di computer ed ogni altro oggetto o supporto utilizzato per archiviare dati riservati, incluse le copie di prova ed i testi manoscritti. In caso di dubbi circa le modalità più opportune per la distruzione e la cancellazione di un supporto con dati personali, non più necessario, rivolgersi al responsabile del trattamento.
3. Adottare adeguati controlli di sicurezza per proteggersi da possibili attacchi da virus. In particolare: accertarsi di essere protetti dal programma antivirus, e comunque attenetevi alle specifiche istruzioni impartite in tema di prevenzione di danni dovuti a programmi abusivi. Ricordarsi che gli antivirus sono in grado di riconoscere solo i codici dei virus pre-programmati. Ricordarsi che qualsiasi supporto registrato il cui contenuto è ignoto o sul quale non sia stato effettuato il controllo antivirus, può essere una sorgente di contaminazione. Anche nuovi programmi, forniti da fabbricanti o distributori autorizzati, possono essere sorgente di contaminazione.
4. In caso di dubbio, rivolgersi all'autorizzato delegato o al responsabile del trattamento.
5. Per questa ragione è indispensabile che tutti i dati personali, trattati nel corso dell'attività di autorizzato, vengano salvati su una cartella apposita, messa a disposizione nel server scolastica.

Utilizzando la cartella a disposizione presso il server, esso provvede infatti automaticamente alla realizzazione delle copie di salvataggio e previene possibili danneggiamenti o corruzioni dei dati, che fossero residenti soltanto sull'hard disk del personal computer locale.

6. Sull'hard disk del proprio dispositivo non possono essere salvati dati personali o comunque non afferenti all'attività scolastica.
7. In caso di dubbio sull'applicazione di questa istruzione, rivolgersi al Responsabile del trattamento.
8. Per ogni cambiamento di mansione o profilo di accesso ai dati, prendere contatto con il proprio Responsabile per la costruzione di un idoneo profilo di autorizzazione.
9. Se vi è necessità di asportare dall’archivio documenti contenenti dati personali, controllare la integrità (che non manchino fogli) e custodirli con diligenza, senza lasciarli abbandonati e non consentendo a terzi non autorizzati di esaminarli o, peggio, copiarli.
6. Ricordarsi che la sicurezza è una condizione operativa alla quale tutti debbono dare un contributo. La robustezza di una maglia condiziona la robustezza della intera catena; pertanto è preciso dovere segnalare immediatamente all'incaricato delegato od al responsabile del trattamento qualsiasi infrazione alle regole di sicurezza e qualsiasi situazione che possa anche potenzialmente alterare il livello predeterminato di sicurezza del trattamento di dati personali.

II.1.1 Altre raccomandazioni afferenti al trattamento con strumenti elettronici

- Non lasciare visualizzati sullo schermo dei dati personali, in vostra assenza; attivare, se disponibile, la funzione di screensaver sotto password, che permette di ripristinare assai rapidamente la connessione sospesa. In alternativa, compatibilmente con le esigenze di sicurezza ambientali, si raccomanda di effettuare la disconnessione del personal computer dal server, prima di lasciare l'apparato incustodito per un periodo apprezzabile. Ricordare che ove un'attività venga svolta dal proprio terminale, attivo ed abilitato secondo il vostro codice identificativo personale, essa viene automaticamente addebitata all'incaricato, del quale è stato utilizzato il codice identificativo personale.
- Accertarsi che estranei non possano osservare i dati sullo schermo, ad esempio attraverso le pareti vetrate di un corridoio.
- Evitare di discutere, anche con i colleghi, informazioni relative a dati personali, se non attinenti al lavoro che dovete svolgere.
- Cancellare sempre tutti i dati residui presenti nel computer, quando non più utilizzati; asportare tutti fogli stampati prodotti dalla stampante, e portare via l'originale, messo nella fotocopiatrice.
- Se ci si accorge di aver accesso a dati e programmi di trattamento non di propria competenza, informare subito il titolare o il responsabile.
- Non utilizzare dischetti con dati e programmi di provenienza ignota, per evitare infezioni da virus nel computer e di danneggiare i dati.
- Al termine del trattamento, chiudere sempre i programmi secondo le appropriate procedure di sicurezza.
- Proteggere sempre i computer, gli apparati terminali ed i supporti di registrazione da condizioni climatiche avverse.

III. Il trattamento di dati personali senza l'ausilio di strumenti elettronici

Poiché i rischi di perdite, danneggiamento e comunicazione non autorizzata di dati personali sono presenti anche nel caso i dati non siano conservati in sistemi informativi, ma si trovino ad esempio archiviati su supporti cartacei, indichiamo di seguito specifiche modalità tecniche da adottare, in caso di trattamento con strumenti diversi da quelli elettronici.

- Dal luogo sicuro devono essere asportati solo i documenti strettamente necessari per le operazioni trattamento e non intere pratiche, se ciò non è necessario
- Al termine delle operazioni di trattamento, i documenti devono essere immediatamente riposti nel luogo sicuro
- Per tutto il periodo in cui i documenti sono all'esterno del luogo sicuro, l'autorizzato non deve mai perderli di vista, adempiendo ad un preciso obbligo di custodia dei documenti stessi. A questo proposito, si presti particolare attenzione ai casi di allontanamento temporaneo dell'ufficio, lasciando le pratiche sul tavolo. È comportamento diligente e prudenziale quello di tenere le pratiche sempre sott'occhio, o, dovendosi allontanare, riporre le stesse in un contenitore protetto
- L'incaricato deve inoltre controllare che i documenti, composti da numerose pagine o più raccoglitori, siano sempre completi, verificando che sia il numero dei fogli che la integrità del contenuto, rispetto a quanto presente, all'atto del prelievo dal luogo sicuro

- Se si debbono abbandonare, ad esempio di sera, in ufficio o al termine dell'orario di lavoro, gli anzidetti documenti, l'incaricato deve identificare un luogo sicuro di custodia che dia sufficienti garanzie di protezione da accessi non autorizzati (un armadio chiuso a chiave, un cassetto chiuso a chiave, una cassaforte, un armadio blindato, un classificatore chiuso a chiave); ove si utilizzi un contenitore chiuso a chiave, di qualunque natura, occorre accertarsi che non esistano duplicati abusivi delle chiavi e che tutte le chiavi siano in possesso solo di incaricati autorizzati
- Ci si deve in particolare accertare che un visitatore o terzo (addetto alla manutenzione, addetto alle pulizie, collega non autorizzato) possa entrare in ufficio anche non invitato o per cause accidentali, non possa venire a conoscenza dei contenuti dei documenti (attenzione alla lettura alla rovescia!)
- Si deve limitare al minimo assoluto il numero di fotocopie effettuate.
- Si deve adottare una prassi per la consegna delle copie ai destinatari, che dia tutte le garanzie di sicurezza, in particolare utilizzando buste di sicurezza sigillate, oppure effettuando la consegna personalmente, di modo da ridurre al minimo la possibilità che soggetti terzi non autorizzati possano prendere visione del contenuto, o addirittura fotocopiarlo all'insaputa del mittente e destinatario
- Particolare cautela deve essere presa ove i documenti in questione vengano consegnati in originale a un autorizzato o responsabile, per evitare possibili perdite o distruzione accidentale
- Documenti contenenti dati particolari o dati che, per una qualunque ragione, siano stati indicati dal responsabile come meritevoli di particolare attenzione, in fase di affidamento, devono essere custoditi con misure più spinte, rispetto a quelle sinora indicate (per eventuali ulteriori informazioni, rivolgersi al responsabile).
- Quale che sia il tipo di spedizione adottato, ci si accerti che esso consenta di avere prova certa del fatto che il destinatario abbia effettivamente ricevuto i documenti inviati e che essi sono giunti integri, e quindi non manomessi o alterati in fase di trasporto (sigilli);
- Eventuali fotocopie non riuscite bene debbono essere distrutte in un apposito distruggitore, se disponibile, oppure devono essere strappate in pezzi talmente piccoli, da non consentire in alcun modo la ricostruzione del contenuto, che deve essere comunque illeggibile
- È tassativamente proibito trasportare all'esterno del posto di lavoro fotocopie non riuscite, da utilizzare altrove come carta per appunti
- Quando i documenti devono essere trasportati all'esterno del luogo di lavoro, l'incaricato deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti; deve inoltre evitare che sia possibile esaminare, da parte di un soggetto terzo non autorizzato, anche solo la copertina del documento in questione
- Durante il trasporto, la cartella non deve essere mai lasciata incustodita e preferibilmente deve essere tenuta chiusa a chiave o devono essere azionate le serrature a combinazione di presenti sulla cartella o valigia
- È tassativamente proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il corrispondente sia un incaricato, il cui profilo di autorizzazione sia tale da potere trattare i dati in questione
- Si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando cellulari all'esterno della scuola, in presenza di terzi

non autorizzati, per evitare che dati personali possano venire a conoscenza di terzi non autorizzati, anche accidentalmente. Queste precauzioni diventano particolarmente importanti quando il telefono è utilizzato in luogo pubblico o aperto al pubblico

- Si faccia molta attenzione all'utilizzo di macchine fotocopiatrici di ultima generazione, che possono catturare l'immagine del documento, memorizzarlo su hard disk inserito all'interno della macchina, e successivamente stamparla, talvolta conservando file elettronico del documento. In questo caso la fotocopiatrice non va classificata come strumento non elettronico, ma come strumento elettronico, e a tutti gli effetti si applicano pertanto le particolari cautele, previste per questa tipologia di strumenti
- In caso di dubbio sulle modalità di applicazione di quanto sopra illustrato, o per chiedere ulteriori chiarimenti in merito, l'incaricato deve rivolgersi al proprio titolare o responsabile.
- Può capitare assai spesso che documenti cartacei contenenti dati personali, anche sensibili, vengano inseriti in una busta ed abbandonati sul sedile di una autovettura, che talvolta viene lasciata incustodita anche per lungo tempo. Inoltre, può capitare che tali dati vengano inseriti nella borsetta, dove si trova anche un borsellino od un telefono cellulare, che possono rappresentare un attraente bersaglio per uno scippatore.
- Le stesse preoccupazioni valgono per i dati che vengono riversati su un personal computer portatile, che viene trasportato fuori dalla scuola, lasciato talvolta incustodito in condizioni tali che un attaccante, debitamente preparato, potrebbe esser in condizione di estrarre da questo computer dati, che la legge vuole siano tutelati con particolare attenzione. Ecco perché la legge si preoccupa di dare specifiche indicazioni, in merito al fatto che ad esempio una pennetta usb, un CD-ROM o altri supporti informatici, nonché i documenti su supporto cartaceo, vengano debitamente protetti in fase di trasporto. Per dati ad alto rischio, come i dati sensibili genetici, si prescrive perfino l'utilizzo di un contenitore con serratura, che potrebbe anche essere una borsa con un lembo di chiusura protetto da una serratura a codice o da chiave, oppure con altri accorgimenti, come ad esempio una busta sigillata, che mette in immediata evidenza una possibile violazione.

Indipendentemente dallo strumento specifico di protezione dei dati, è indispensabile che l'autorizzato, che occasionalmente o sistematicamente trasporta questi dati, archiviati su qualsiasi tipo di supporto, presti particolare attenzione, non abbandonando mai i dati stessi ed accertandosi che essi non siano, in alcun modo, accessibili a terzi estranei.

IV. Raccomandazioni in fase di comunicazione dei dati personali

- Se un visitatore vi chiede di fare una telefonata, componete voi il numero e passate il telefono al visitatore
- Se vengono richiesti via telefono dati personali, accertarsi sempre che il richiedente abbia titolo a richiederli. In caso di dati sensibili od in circostanze particolari, valutate la possibilità di utilizzare mezzi più sicuri di comunicazione dei dati
- Quando si deve comunicare dati personali via telefono, accertarsi che terzi estranei nelle vicinanze non possano udirli

· Prima di inviare ad un corrispondente un fax con dati personali, accertarsi che sia pronto a riceverli e che non vengano abbandonati presso la macchina ricevente, in attesa di essere prelevati

V. La Posta Elettronica

5.1. La Posta Elettronica è uno strumento di lavoro

L'utilizzo della posta elettronica scolastica è connesso allo svolgimento dell'attività lavorativa. L'uso per motivi personali deve essere moderato ed è tollerato esclusivamente ai sensi dell'articolo seguente. I Responsabili/Autorizzati/Incaricati/Designati possono avere in utilizzo indirizzi nominativi di posta elettronica.
Le caselle e-mail possono meglio essere assegnate con natura impersonale (tipo info, amministrazione, fornitori, direttore, collaboratore, consulenza, …) proprio per evitare ulteriormente che il destinatario delle e-mail possa considerare l'indirizzo assegnato al dipendente "privato", ai sensi dei suggerimenti del Garante a tal proposito.
I Responsabili assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

5.2. Misure Preventive per ridurre utilizzi illeciti della Posta Elettronica

L'Istituzione Scolastica è consapevole della possibilità di un limitato utilizzo personale della posta elettronica da parte dei Responsabili/Autorizzati/Incaricati/Designati e allo scopo prevede le seguenti misure:
1. In caso di ricezione sull'e-mail scolastica di posta personale, si avverte di cancellare immediatamente ogni messaggio, al fine di evitare ogni eventuale e possibile back up dei dati.
2. Avvisare l'Istituzione Scolastica quando alla propria posta personale siano allegati files eseguibili e/o di natura incomprensibile o non conosciuta.

5.3. Divieti Espressi

1. È vietato utilizzare l'indirizzo di posta elettronica contenente il nome di dominio dell'Istituzione Scolastica per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta dell'Istituzione Scolastica, nonché utilizzare il dominio dell'Istituzione Scolastica per scopi personali.
2. È vietato scrivere e generare messaggi di posta elettronica utilizzando l'indirizzo scolastica, diretti a destinatari esterni dell'Istituzione Scolastica, senza utilizzare il seguente disclaimer:
«Il presente messaggio e gli eventuali suoi allegati sono di natura scolastica, prevalentemente confidenziale e sono visionabili solo dal destinatario di posta elettronica. La risposta o l'eventuale invio spontaneo da parte vostra di e-mail al nostro indirizzo potrebbero non assicurare la confidenzialità potendo essere viste da altri soggetti appartenenti all'Istituzione Scolastica oltre al sottoscritto, per finalità di sicurezza informatica, amministrative e allo scopo del continuo svolgimento dell'attività scolastica. Qualora questo messaggio vi fosse pervenuto per errore, vi preghiamo di cancellarlo dal vostro sistema e vi chiediamo di volercene dare cortesemente comunicazione al mittente".
3. È vietato creare, archiviare o spedire, anche solo all'interno della rete scolastica, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo scolastica.
4. È vietato trasmettere messaggi a gruppi numerosi di persone (es. a tutto un ufficio o ad un'intera divisione) senza l'autorizzazione necessaria.
5. È vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.
6. È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'Istituzione Scolastica informazioni riservate o comunque documenti scolastici, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.
7. È vietato utilizzare la posta elettronica per messaggi con allegati di grandi dimensioni.

Nella definizione delle regole d'uso del servizio di posta elettronica e delle modalità di controllo, il MIM ritiene di grande importanza salvaguardare la libertà di espressione e di pensiero e la garanzia della privacy dell'individuo. Questa Politica rispetta quindi i principi basilari esposti, nel contesto delle obbligazioni legali e delle politiche di sicurezza dell'Amministrazione.
L'Amministrazione, anche sulla base delle direttive del governo tese a promuovere la crescita delle comunicazioni in formato digitale e l'abbattimento di quelle cartacee, considera la posta elettronica uno strumento fondamentale, che viene messo a disposizione di tutti coloro che ne abbiano diritto. La presente politica vale anche come informativa sulle finalità e modalità del trattamento dei dati personali, ricavabili dalle attività di controllo tecnico svolte sul servizio di posta elettronica, ai sensi degli art. 13 e 14 del Reg UE 679/2016

Le condizioni di utilizzo della casella di posta elettronica xy.zw@istruzione.it, fissate dal MIM, sono le seguenti:

a. Finalità del servizio di posta elettronica. Il MIM incoraggia l'uso della posta elettronica per scambiare informazioni, migliorare le comunicazioni, scambiare idee e per rendere più efficaci ed efficienti i processi di lavoro a supporto della missione istituzionale dell'Amministrazione.

b. Proprietà del MIM: il servizio di posta elettronica del MIM, erogato per il tramite dei Fornitori dei servizi in outsourcing, è proprietà del MIM, pertanto ogni casella di posta elettronica associata al Ministero (nel dominio istruzione.it) o a suoi uffici o assegnata a individui o funzioni del Ministero, sono di proprietà del MIM.

c. Oneri a carico dell'Utente. Il servizio di posta elettronica è attivato, qualora ne abbia diritto, su richiesta dell'Utente ed è gratuito; resta a carico dell'Utente l'onere di dotarsi della strumentazione tecnica necessaria per accedere al Servizio, ivi compresa l'eventuale spesa connessa al traffico telefonico sostenuto. Per usufruire del servizio è necessario registrarsi. Con la registrazione, l'Utente dichiara di aver letto e accettato tutti i termini e le condizioni di utilizzo del Servizio indicate nel documento. In mancanza dell'accettazione, il servizio non potrà essere attivato. Il MIM fornisce all'Utente che richieda l'attivazione del servizio un codice Utente ed una password modificabile. L'accesso al Servizio è consentito solo mediante tali identificativi.

d. Limitazioni di Responsabilità per il Ministero. Il MIM non può essere ritenuto responsabile per qualsiasi danno, diretto o indiretto, arrecato all'Utente ovvero a terzi e derivante: – dall'eventuale interruzione del Servizio – dall'eventuale smarrimento di messaggi diffusi per mezzo del Servizio – da messaggi inviati/ricevuti o da transazioni eseguite tramite il Servizio – da accesso non autorizzato ovvero da alterazione di trasmissioni o dati dell'Utente.

e. Restrizioni all'uso del servizio. Gli utenti del servizio di posta elettronica sono tenuti ad usarlo in modo responsabile, cioè, rispettando le leggi, la presente e altre politiche e procedure del Ministero e secondo normali standard di cortesia, correttezza, buona fede e diligenza professionale. L'accesso ai servizi di posta elettronica dall'Amministrazione può essere totalmente o parzialmente limitato dall'Amministrazione stessa, senza necessità di assenso da parte dell'utente e anche senza preavviso: quando richiesto dalla legge e in conformità ad essa in caso di comprovati motivi che facciano ritenere la violazione della presente politica o delle disposizioni di legge vigenti al venir meno delle condizioni in base alle quali si ha facoltà di utilizzare il servizio (ad es. cessazione per qualsiasi motivo del rapporto di lavoro con l'Amministrazione) in casi eccezionali, quando richiesto per esigenze operative critiche e improcrastinabili.

a. L'accesso ai servizi di posta elettronica può essere disattivato dall'Amministrazione in caso di cessazione del rapporto di lavoro o di non utilizzo della stessa per un periodo superiore ai 9 mesi, senza necessità di assenso da parte dell'utente. Non è prevista alcuna forma di indennizzo per il venir meno del servizio.

b. Assenso e Conformità. Il MIM è tenuto in generale ad ottenere l'assenso del titolare della casella di posta elettronica prima di ogni ispezione dei messaggi o accesso alle registrazioni o ai messaggi di posta elettronica, fatta eccezione per quanto disposto al

punto g). D'altro canto, ci si attende che il personale del Ministero soddisfi le richieste dell'Amministrazione riguardanti la fornitura di copie delle registrazioni di posta elettronica in suo possesso che riguardino le attività lavorative del Ministero o richieste per soddisfare obblighi di legge, indipendentemente dal fatto che tali registrazioni risiedano o meno su computer di proprietà dell'Amministrazione. Il mancato rispetto di tali richieste può portare all'applicazione delle condizioni di cui la punto g).

c. Limitazioni all'accesso senza assenso. Il MIM non ispeziona e non accede ai messaggi di posta elettronica dell'utente senza la sua autorizzazione. D'altro canto, il Ministero potrà permettere l'ispezione, il monitoraggio o l'accesso alla posta elettronica degli utenti, anche senza l'assenso del titolare, solamente nei seguenti casi:

- su richiesta scritta dell'autorità giudiziaria nei casi previsti dalla normativa vigente
- previo preavviso all'utente, per gravi e comprovati motivi[1], che facciano credere che siano state violate le disposizioni di legge vigenti o le politiche del MIM in materia di sicurezza
- per atti dovuti[2];
- in situazioni critiche e di emergenza[3].

d. Registro elettronico. L'Amministrazione registra e conserva, in forma anonima, i dati delle caselle di posta elettronica messe a disposizione dei propri utenti, tramite scrittura in appositi file di log, delle seguenti informazioni minime per ogni messaggio:

- mittente
- destinatario/i
- giorno ed ora dell'invio
- esito dell'invio.
- I file di registro sono conservati per un periodo di due anni.

AVVERTENZE

Gli utenti del servizio di posta elettronica sono avvisati del fatto che:

1. La natura stessa della posta elettronica la rende meno sicura di quanto si possa immaginare. Ad esempio, i messaggi di posta elettronica spediti ad una persona possono essere facilmente inoltrati ad altri destinatari. Il Ministero non può proteggere gli utenti da fatti come quelli descritti che esulano dalle proprie possibilità e compiti. Gli utenti pertanto devono esercitare la massima cautela nell'uso della posta elettronica per comunicare informazioni riservate o dati sensibili.

---

[1]**Grave e comprovato motivo**: evidenza oggettiva, non basata quindi su semplici sospetti o illazioni, che dimostra l'avvenuta violazione di disposizioni di leggi vigenti o delle politiche di sicurezza dell'Amministrazione.

[2]**Atti dovuti**: circostanze in base alle quali la mancanza di adeguate azioni può comportare danni significativi a cose o persone, perdita di informazioni di rilievo per l'Amministrazione o danni economici e di immagine per l'Amministrazione e per le persone che ne fanno parte.

[3]**Situazioni critiche o di emergenza**: circostanze in cui la tempestività d'azione è di fondamentale importanza al fine di evitare danni significativi a cose o persone, perdita di informazioni di rilievo per l'Amministrazione o danni economici e di immagine per l'Amministrazione e per le persone che ne fanno parte o l'interruzione dei servizi informatici e la continuità operativa dei processi

2. I messaggi di posta elettronica, creati e conservati sia su apparati elettronici forniti dall'Amministrazione che su altri sistemi, possono costituire registrazioni di attività svolte dall'utente nell'espletamento delle sue attività lavorative. È possibile quindi che venga richiesto di accedere ai contenuti dei messaggi per un eventuale utilizzo nell'ambito di contenziosi che coinvolgano l'Amministrazione. Il MIM non darà corso automaticamente a tutte le richieste di accesso, ma le valuterà in relazione a precisi obblighi di legge quali la privacy ed altre normative applicabili. Gli utenti devono però tener presente che, per quanto detto, in nessun caso l'Amministrazione può garantire che non saranno accedute informazioni personali degli utenti presenti in messaggi di posta elettronica residenti sui sistemi dell'Istruzione.

3. Il MIM, in generale, non può e non intende porsi come valutatore dei contenuti dei messaggi di email scambiati, né può proteggere gli utenti dalla ricezione di messaggi che possano essere considerati offensivi. Gli utenti sono comunque fortemente incoraggiati a usare nella posta elettronica le stesse regole di cortesia che adopererebbero in altre forme di comunicazione.

4. Non c'è garanzia, a meno di utilizzare sistemi di posta certificata, che i messaggi ricevuti provengano effettivamente dal mittente previsto, perché è piuttosto semplice per i mittenti mascherare la propria identità, anche se ciò costituisce, tra le altre cose, una violazione della presente politica. Inoltre i messaggi di posta che arrivano come "inoltro" di precedenti messaggi, potrebbero essere stati modificati rispetto all'originale. Pertanto, in caso di dubbi, chi riceve un messaggio di posta elettronica dovrebbe verificare con il mittente l'autenticità delle informazioni ricevute.

USO CONSENTITO

L'uso del servizio di posta elettronica del MIM è soggetto alle seguenti condizioni:

a. Proibizioni. È fatto divieto a tutti gli utenti di utilizzare il servizio di posta elettronica per inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione del MIM. È inoltre vietato l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali e la fornitura (gratuita o a pagamento) a persone fisiche o giuridiche di qualsiasi lista o elenco degli Utenti del Servizio. È proibito fornire le proprie credenziali di accesso a sistemi o procedure, così come rispondere a messaggi email che facciano richiesta di questo tipo di informazioni. Chiunque riceva comunicazioni della natura sopra indicata dovrà segnalarlo alla Direzione Generale per i contratti, gli acquisti e per i sistemi informativi e la statistica utilizzando i servizi di assistenza online accessibili attraverso il sito Internet del MIM.

b. Uso Personale. È consentito l'utilizzo ragionevole del proprio account nel dominio "istruzione.it" a fini privati e personali, purché, in aggiunta a quanto indicato nei punti precedenti, tale utilizzo non:

- sia causa, diretta o indiretta di disservizi dei sistemi elaborativi e dei servizi di posta elettronica dell'Amministrazione;
- sia causa di oneri aggiuntivi per l'Amministrazione; o

- interferisca con le attività lavorative dell'utente o con altri obblighi dello stesso verso l'Amministrazione.

L'utente è edotto del fatto che l'Amministrazione considera, ai fini di eventuali ispezioni, tutti i messaggi di posta elettronica da lui gestiti come strettamente afferenti all'uso del servizio per scopi di lavoro. L'Amministrazione presuppone quindi che l'utente decida di utilizzare la posta elettronica per scopi personali avendone preliminarmente e attentamente valutato l'opportunità. Si ricorda comunque che per gli usi personali è possibile dotarsi di una casella di posta elettronica alternativa, ottenibile gratuitamente presso molti fornitori esterni, e liberamente consultabile via internet.

SICUREZZA E RISERVATEZZA

Oltre a quanto indicato ai paragrafi precedenti, gli utenti devono tener presente che, nell'assolvimento dei propri compiti, il personale che gestisce i sistemi di elaborazione e le reti di telecomunicazione può avere, saltuariamente, la necessità di analizzare i dati transazionali dei messaggi di posta per garantire il corretto funzionamento del servizio e in queste occasioni è possibile che avvengano inavvertitamente accessi al contenuto stesso dei messaggi. Tale personale è tenuto comunque al rispetto di stretti vincoli di riservatezza qualora di verificassero i casi citati.

Il Ministero della Pubblica Istruzione si pone come obiettivo fondamentale la fornitura di servizi di posta elettronica sicuri ed affidabili avvalendosi di fornitori altamente qualificati. Va comunque ricordato, come già detto in precedenza, che la sicurezza e riservatezza della posta elettronica non possono essere garantite in ogni circostanza, in particolare per quanto concerne i messaggi di posta scaricati sui Personal Computer.

5.4. Posta Elettronica in caso di assenze programmate ed assenze non programmate

Nel caso di assenza prolungata sarebbe buona norma attivare il servizio di risposta automatica (Auto- reply).

In alternativa, e in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività scolastica, il Responsabile/Autorizzato/Incaricato/Designato deve nominare un collega fiduciario con lettera scritta che in caso di assenza inoltri i file necessari a chi ne abbia urgenza.

Qualora il Responsabile/Autorizzato/Incaricato/Designato non abbia provveduto ad individuare un collega fiduciario o questi sia assente o irreperibile, l'Istituzione Scolastica, mediante personale appositamente responsabile, potrà verificare il contenuto dei messaggi di posta elettronica del responsabile, informandone il responsabile stesso e redigendo apposito verbale.

5.5. Utilizzo Illecito di Posta Elettronica

– È vietato inviare, tramite la posta elettronica, anche all'interno della rete scolastica, materiale a contenuto violento, sessuale o comunque offensivo dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.

– È vietato inviare messaggi di posta elettronica, anche all'interno della rete scolastica, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.

Qualora il Responsabile/Autorizzato/Incaricato/Designato/ riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all'Istituzione Scolastica.

VI. Uso di altri dispositivi (Notebook, Tablet, Cellulare, Smartphone e di altri dispositivi elettronici)

7.1. L'utilizzo del notebook, tablet o smartphone.

Il computer portatile, il tablet e il cellulare (di seguito generalizzati in "dispositivi mobili") possono venire concessi in uso dall'Istituzione Scolastica ai Responsabili che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'Istituzione Scolastica.

Il Responsabile/Autorizzato/Incaricato/Designato è responsabile dei dispositivi mobili assegnatigli dall'Istituzione Scolastica e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai dispositivi mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. In particolare i file creati o modificati sui dispositivi mobili, devono essere trasferiti sulle memorie di massa scolastici al primo rientro in ufficio e cancellati in modo definitivo dai dispositivi mobili (Wiping). Sui dispositivi mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dall'Istituzione Scolastica. I dispositivi mobili utilizzati all'esterno (convegni, visite in altre scuole, in aziende, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto. In caso di perdita o furto dei dispositivi mobili, deve far seguito la denuncia alle autorità competenti. Allo scopo si deve avvisare immediatamente L'Istituzione Scolastica che provvederà – se del caso – ad occuparsi delle procedure connesse alla privacy. Anche di giorno, durante l'orario di lavoro, al Responsabile non è consentito lasciare incustoditi i dispositivi mobili. Al Responsabile è vietato lasciare i dispositivi mobili incustoditi e a vista dentro l'auto o in una stanza d'albergo o nell'atrio dell'albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali.

I dispositivi mobili che permettono l'attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciti privi di PIN.

Laddove il dispositivo mobile sia accompagnato da un'utenza, il Responsabile/Autorizzato/Incaricato/Designato è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati, …) e a rispettarli. Qualora esigenze lavorative richiedessero requirement differenti, il Responsabile/Autorizzato/Incaricato/Designato/ è tenuto ad informare tempestivamente e preventivamente L'Istituzione Scolastica.

In relazione alle utenze mobili, salvo autorizzazione dell'Istituzione Scolastica, è espressamente vietato ogni utilizzo all'estero e anche in caso di autorizzazione dell'Istituzione Scolastica, gli utilizzi all'esterno devono essere preventivamente comunicati all'Istituzione Scolastica per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

7.2. Dispositivi personali (BYOD).

Ai dipendenti non è permesso svolgere la loro attività su PC fissi, portatili, dispositivi personali se non per le finalità descritte di seguito.

Dispositivi ammessi: qualsiasi computer portatile, tablet, e-reader, smartphone;

- I dispositivi devono essere usati a scuola per soli scopi didattici e solo dopo previa autorizzazione esplicita del Dirigente, il quale amministra tempi e necessità di utilizzo di tali apparecchiature.
- È vietato agli studenti ed al personale usare dispositivi di registrazione audio, videocamere o fotocamere (o dispositivi che li prevedano) per registrare media o fare foto a scuola, senza il consenso esplicito dell'interessato, e solo dopo che il Dirigente ne ha autorizzato l'uso.
- Connessione alla rete Wi-Fi dell'Istituzione Scolastica: ogni lavoratore potrà usare la connessione wifi disponibile all'interno dell'Istituzione Scolastica solo per finalità didattiche o, comunque, istituzionali. Chi riceve le credenziali per l'accesso alla rete d'Istituto, avrà cura di conservarle in modo sicuro e l'obbligo di non diffonderle a terzi.
- Anche in considerazione di esigenze didattiche, il Dirigente Scolastico potrà autorizzare le classi aderenti a sperimentazioni in essere, temporaneamente o per l'intero anno scolastico, alla rete Wi-Fi d'istituto.

Nel caso di utilizzo di dispositivi forniti dall'Istituzione Scolastica, è necessario che il dispositivo abbia password di sicurezza stringenti, approvate dall'Istituzione Scolastica e l'eventuale furto o smarrimento del dispositivo deve essere immediatamente segnalato anche all'Istituzione Scolastica, per eventuali provvedimenti di sicurezza.

Al responsabile è vietato l'utilizzo di memorie esterne personali (quali chiavi USB, memory card, cd-rom, DVD, macchine fotografiche, videocamere, tablet, …).

I Responsabili non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri dispositivi personali per memorizzare dati dell'Istituzione Scolastica solo se espressamente autorizzati dall'Istituzione Scolastica stesso e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

Tali dispositivi dovranno essere preventivamente valutati dall'Istituzione Scolastica, per la verifica della sussistenza di misure minime ed idonee di sicurezza.

VII. Controllo e provvedimenti disciplinari

Il controllo

L'Istituzione Scolastica, in qualità di Titolare degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

- Tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati.
- Evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo.
- Verificare la funzionalità del sistema e degli strumenti informatici.

12.1. Conseguenze delle infrazioni disciplinari

Le infrazioni disciplinari alle norme del presente Disciplinare Interno potranno essere punite, a seconda della gravità delle mancanze, in conformità alle disposizioni di legge e/o del Contratto Collettivo Nazionale del Lavoro applicato, tra cui:

- Il biasimo inflitto verbalmente.
- Lettera di richiamo inflitto per iscritto.
- Multa.
- La sospensione dalla retribuzione e dal servizio.
- Il licenziamento disciplinare e con le altre conseguenze di ragioni e di legge;

Per i dirigenti valgono le vigenti norme di legge e/o di contrattazione collettiva, fermo restando che, per le violazioni di maggior gravità l'Amministrazione potrà procedere al licenziamento del dirigente autore dell'infrazione.

12.2. Modalità di Esercizio dei diritti

Il lavoratore interessato del trattamento dei dati effettuato mediante strumenti informatici ha diritto di accedere, ai sensi dell'art. 15 del Regolamento, alle informazioni che lo riguardano scrivendo al Titolare dell'Istituzione Scolastica.

VIII: Validità, aggiornamento ed affissione

13.1. Validità

Il presente Disciplinare ha validità a partire dal .....

13.2. Aggiornamento

Il presente Disciplinare sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi dell'Istituzione Scolastica o in caso di mutazioni legislative.

Ogni variazione del presente Disciplinare sarà comunicata ai Responsabili/Autorizzati/Incaricati/Designati.

13.3. Affissione

Il presente Disciplinare verrà pubblicato all'Albo Digitale, ai sensi dell'art. 7 della legge 300/70 e del CCNL.