Regolamento per l'utilizzo degli Strumenti Informatici, posta elettronica e internet, nonché per il trattamento delle informazioni

1. RIFERIMENTI NORMATIVI E DOCUMENTALI

1.1. DOCUMENTI INTERNI

- **Procedura Data Breach**
- **Istruzioni Operative GDPR per Autorizzati**

1.2. NORMATIVA ITALIANA

- **Regolamento Generale sulla Protezione dei Dati personali (Regolamento UE 2016/679)**
- **Decreto Legislativo 30 giugno 2003, n. 196 e successive integrazioni e modificazioni ("Codice in materia di protezione dei dati personali")**
- **Legge 20 maggio 1970, n. 300**, norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e nell'attività sindacale nei luoghi di lavoro e norme sul collocamento (detta anche "statuto dei lavoratori").
- **Codice Civile**

  - Art. 2049 Responsabilità indiretta dell'imprenditore;

  - Art. 2086 Direzione e gerarchia nell'impresa;

  - Art. 2087 Tutela dell'integrità fisica e della personalità morale dei dipendenti, da parte dell'imprenditore;

  - Art. 2104 Diligenza del dipendente nel rispetto delle disposizioni impartite dall'imprenditore.
- **Provvedimenti dell'Autorità Garante per la protezione dei dati personali**

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

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

2. Postazioni di Lavoro

Nella postazione di lavoro sono presenti una serie di informazioni, spesso riservate, che sono facilmente riproducibili, sottraibili o alterabili.

Di conseguenza bisogna attenersi ad una serie di comportamenti, considerati sicuri:

- Nel caso in cui ci si allontani, i terminali devono essere sempre lasciati bloccati (solo l'utente specifico o un amministratore del sistema potranno accedervi).
- La documentazione classificata come riservata, e in generale tutta la documentazione contenente dati personali, non deve mai essere lasciata incustodita. A fronte di un'assenza prolungata è bene non lasciare la documentazione in vista (usare gli armadi e/o cassettiere).
- Gli appunti di lavoro, le bozze di documenti, riferimenti di persone, minori e genitori degli alunni sono sempre da considerarsi riservati e di conseguenza non dovrebbero essere lasciati incustoditi. Tutta la

documentazione deve essere riposta all'interno dei faldoni assegnati al personale e i faldoni devono essere conservati nelle apposite cassettiere/armadi.

- È responsabilità degli utenti autorizzati la conservazione degli strumenti resi disponibili per l'esecuzione delle attività di lavoro negli appositi cassettiere/armadi.

Prima di ogni pausa riordinare la scrivania attenendosi alle norme sopraccitate. Alla fine della giornata lavorativa la postazione di lavoro e la scrivania devono essere "pulite".

3. Utilizzo del Personal Computer

Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screensaver con la relativa password.

3.1. Credenziali di accesso all'elaboratore

L'accesso all'elaboratore è protetto da credenziali di accesso (USERNAME – PASSWORD) che vengono comunicate dal Responsabile Sistemi Informativi/Responsabile IT all'assunzione e che devono essere custodite dall'incaricato con la massima diligenza e non divulgate.

Al primo accesso al proprio account, il personale è tenuto a impostare una nuova password; la password deve essere composta rispettando i seguenti criteri di complessità:

- Non può contenere parti dell'username o del nome completo utente più lunghe di 3 caratteri.
- Deve contenere almeno un carattere che rientri in 3 delle seguenti 4 categorie:
  - lettere maiuscole
  - lettere minuscole
  - numeri
  - simboli

Le password devono essere reimpostate almeno ogni 90 giorni.

La password deve essere immediatamente sostituita, nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di un altro utente, è tenuto a darne immediata notizia al Responsabile IT, al Dirigente Scolastico o al DSGA.

<u>Accesso agli Account in caso di assenza prolungate</u>

Il Responsabile IT o dei Sistemi Informativi può accedere agli account personali per permettere all'Istituto scolastico, titolare del trattamento, di accedere ai dati trattati da ogni incaricato esclusivamente al fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività istituzionale nei casi in cui si renda indispensabile e indifferibile l'intervento (es. prolungata assenza od impedimento dell'incaricato). In queste casistiche il Responsabile dei Sistemi Informativi, previo avviso al dipendente, accede al suo account resettando la password di accesso al fine di recuperare le informazioni necessarie. Al termine dell'intervento il

Responsabile dei Sistemi Informativi deve resettare nuovamente la password in modo che l'utente sia obbligato ad inserirne una nuova al primo accesso.

3.2. Installazione applicativi Software e Gestione impostazioni (non si applica per gli ambienti di test).

Le postazioni di lavoro vengono configurate dal Responsabile dei Sistemi Informativi che si occupa di installare tutti gli applicativi software necessari per lo svolgimento delle mansioni.

Non è consentito installare autonomamente programmi provenienti dall'esterno salvo autorizzazione esplicita del Titolare del trattamento e del Responsabile dei sistemi informativi, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Istituto scolastico a gravi responsabilità civili e anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L.248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema, di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita del Responsabile IT.

3.3. Utilizzo dispositivi portatili (Notebook, Tablet e Smartphone)

Il personale scolastico è responsabile degli eventuali dispositivi portatili assegnati (pc, tablet, USB, etc.) e devono custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai Notebook si applicano le regole di utilizzo previste per i Personal Computer in rete.

Tutti i dispositivi portatili assegnati agli utenti devono essere trattati secondo le specifiche del produttore, trasportandoli nelle apposite custodie e avendone particolare cura in termini di conservazione del bene.

L'utilizzo dei dispositivi al di fuori della sede scolastica, pur garantendo i livelli minimi di sicurezza, può presentare maggiori rischi e di conseguenza è necessario prestare maggiore attenzione.

Nello specifico i dispositivi portatili utilizzati all'esterno devono essere custoditi a cura dell'utente in luoghi protetti da minacce quali:

- Furto
- Danneggiamento Esterno Volontario/Involontario
- Minacce ambientali (allagamento, incendio)
- Accessi non Autorizzati

Al fine di evitare accessi non autorizzati ai dati dei dispositivi portatili, in caso di non utilizzo è necessario disattivare sistemi di connessione wireless (WLAN/Wi-Fi, Bluetooth) e, ove possibile e pertinente, proteggere i dispositivi con antivirus aggiornati e/o firewall, specialmente all'esterno (access point pubblici).

In caso di smarrimento/sottrazione è necessario dare tempestiva comunicazione al Responsabile della Protezione dei Dati dell'Istituto scolastico e al Responsabile dei sistemi Informativi.

È responsabilità dell'utente rimuovere tutte le informazioni dal dispositivo portatile prima della riconsegna.

4. Utilizzo della rete Istituto scolastico

4.1. Salvataggio File nelle unità di rete

Le unità di rete sono aree di condivisione di informazioni strettamente ad uso lavorativo e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere salvato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.

È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente, così come è vietato utilizzare sistemi in cloud (es. dropbox o similari) per l'archiviazione dei dati non autorizzati dal Dirigente Scolastico o dal Responsabile dei sistemi informativi.

Il Responsabile dei sistemi informativi, può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC del personale preposto ad operazioni di trattamento sui dati personali (incaricati) sia sulle unità di rete.

Costituisce buona regola la periodica pulizia degli archivi (almeno ogni sei mesi), con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

L'Istituto scolastico favorisce la piena connettività nella Rete Intranet ed Internet delle risorse operanti per suo conto; tuttavia, per ottimizzare l'efficienza e la sicurezza del trattamento dei dati personali, ogni utilizzatore di postazione fissa dovrà attenersi alle prescrizioni indicate nel presente Regolamento, consapevole che il titolare dell'informazione (attraverso una funzione specifica dei servizi informatici, anche mediante soggetti esterni), per garantire la piena sicurezza della rete o per motivi di manutenzione ovvero per garantire la continuità dello svolgimento dei servizi forniti ai clienti e dell'attività lavorativa, si riserva di superare ogni accesso e limitazione predisposta (ad esempio password, E-Mail, dischi di rete).

Nel caso sia previsto un accesso remoto alle informazioni dell'Istituto scolastico, lo stesso deve essere effettuato tramite autenticazione e utilizzando strumenti tecnologici adeguati e approvati dal Responsabile dei Sistemi Informativi (es. VPN). Nell'utilizzo dei sistemi dell'Istituto scolastico da remoto, inoltre, è indispensabile valutare l'ambiente in cui ci si trova (al fine di evitare che persone non autorizzate vengano a conoscenza di informazioni riservate in maniera accidentale).

4.2. Utilizzo delle stampanti di rete

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

4.3. Uso della rete Internet e dei relativi servizi

Il Personal Computer abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa o alle finalità istituzionali dell'Istituto scolastico.

La rete Internet, infatti, rappresenta una risorsa fondamentale per le attività dell'Istituto scolastico e il suo utilizzo da parte dei dipendenti è essenziale per il corretto svolgimento di tali attività. Nel contempo però tale risorsa può rappresentare anche una minaccia per la sicurezza delle informazioni dell'Istituto scolastico. Infatti nell'underground tecnologico di Internet si possono incontrare facilmente (tramite la semplice navigazione o il download di file) minacce che possono compromettere la riservatezza e la disponibilità delle informazioni

dell'Istituto scolastico. Si parla di Malware in generale (es. i CryptoLocker), ma anche di pagine web infette come veicolo di tale software malevolo.

Per tale ragione il dipendente deve limitare l'uso di tale rete esclusivamente ai fini lavorativi ed evitare l'accesso a risorse web di dubbia sicurezza e utilità per l'Istituto scolastico.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet.

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 Dirigente Scolastico o dal DSGA e con il rispetto delle normali procedure di acquisto.

È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum non istituzionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

È vietato l'utilizzo di strumenti per il file sharing e per download massivo di file (rapidshare, filestube, P2P, …).

L'utilizzo dei Social Network è consentito nei limiti dell'utilizzo istituzionale ed in ogni caso non è concessa la pubblicazione di informazioni la cui distribuzione sia ad uso interno o riservata ovvero non sia stata autorizzata.

L'Istituto scolastico, al fine di prevenire determinate operazioni non consentite, potrebbe implementare dei sistemi di filtro della navigazione che puntano a mitigare i rischi alla sicurezza dell'Istituto scolastico; ciononostante la prima e più efficace misura di sicurezza è rappresentata dalla consapevolezza dell'utente. Nel caso in cui un evento dannoso o una situazione di pericolo non siano stati impediti con preventivi accorgimenti tecnici, l'Istituto scolastico adotterà eventuali misure che consentano la verifica di comportamenti anomali, attraverso le modalità e le procedure di seguito specificate

L'Istituto scolastico potrebbe attivare, infatti, sistemi di monitoraggio della navigazione secondo le previsioni di cui al Provvedimento del Garante in materia di trattamento dati personali, (Provvedimento del 1 marzo 2007), effettuando un controllo generalizzato e anonimo dei log di connessione. Pertanto, in seguito al rilevamento di anomalie nel sistema dei dati, per motivi di manutenzione o in caso di comportamenti anomali individuati in una determinata area o a seguito di controlli a campione saltuari, l'Istituto scolastico potrà attivare meccanismi di monitoraggio delle attività di rete (file di log) e di controllo del traffico Internet o del traffico della posta elettronica o dei file di back up per fini organizzativi o di manutenzione, per verifiche sulla funzionalità del sistema o di controllo della sicurezza dell'impianto. Gli archivi di log risultanti da questo monitoraggio, effettuati in determinate aree dell'Istituto scolastico e allo stesso tempo sufficientemente grandi da garantire la riservatezza dei lavoratori, contengono traccia di ogni operazione di collegamento effettuata dall'interno dell'Istituto scolastico verso Internet.

In caso di accertata violazione definita tramite alert, il Responsabile dei Sistemi Informativi provvederà prontamente a segnalare l'attività illecita riscontrata mediante una comunicazione rivolta a tutti i dipendenti.

In rispetto al principio di finalità, pertinenza e non eccedenza, tali log vengono tenuti negli archivi dell'Istituto scolastico per un breve periodo e può accedere a tali informazioni solo il Responsabile dei Sistemi Informativi.

Un eventuale prolungamento dei tempi di conservazione di tali log, rispetto a quelli stabiliti, è da considerarsi come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;

- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

5. Uso della posta elettronica

La posta elettronica rappresenta uno dei principali strumenti di comunicazione a disposizione del dipendente. La sua immediatezza e disponibilità anche su dispositivi portatili, unitamente al basso costo di esercizio la rendono particolarmente efficace. I rischi connessi all'uso della posta sono legati principalmente alla tipologia dei dati che in essa transitano e alla loro comunicazione/diffusione. Il livello di riservatezza di un messaggio di posta elettronica semplice, infatti, si avvicina più a quello di una lettera aperta (cartolina postale) che a quello di una lettera chiusa.

La casella di posta, assegnata dall'Istituto scolastico all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse per i soli fini lavorativi.

Si rende noto, in proposito, che per motivi organizzativi e funzionali, l'Istituto scolastico archivia tutti i messaggi di posta elettronica, in uscita ed in entrata (anche nelle copie di back up). Conseguentemente, stante la natura di strumento di comunicazione istituzionale del sistema di posta elettronica, l'utilizzatore è consapevole che sullo stesso non potrà essere garantita la riservatezza dei documenti inviati e ricevuti; pertanto, sarà impegno del dipendente evitare l'utilizzo delle caselle di posta elettronica per comunicazioni di carattere personale o che esulino dal contesto istituzionale cui sono preposte.

È fatto divieto di utilizzare le caselle di posta elettronica dell'Istituto scolastico per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.

L'invio di comunicazioni elettroniche con informazioni personali è sottoposto alla disciplina prevista dal Regolamento UE 2016/679 e il Decreto Legislativo 30 giugno 2003 n. 196 come revisionato e uniformato alla normativa europea. Le comunicazioni riservate / confidenziali via mail, pertanto, devono segnalate tramite apposito TAG [CONFIDENZIALE] nell'oggetto ed è fatto divieto l'inoltro a personale diverso da chi l'ha ricevuta senza preventiva autorizzazione da parte del Titolare o delle Direzione.

Il personale che riceve per via elettronica documenti/informazioni riservate non può in alcun caso inviarle o metterle comunque a conoscenza di personale non autorizzato.

Il personale che invia messaggi di posta elettronica a destinatari diversi (es. comunicazioni alle famiglie) deve inserire i relativi indirizzi in "ccn" e non in "cc".

Le informazioni/documenti riservati possono essere stampate solo in caso di necessità, i documenti cartacei riportanti informazioni di origine elettronica riservate devono essere distrutti nel momento in cui termini la loro funzione.

E' fatto divieto in ogni caso di divulgare a soggetti non autorizzati le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal segreto cui sono tenuti i dipendenti in ottemperanza agli obblighi di fedeltà e correttezza.

È consigliabile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (posta, posta elettronica certificata, etc.).

Per la trasmissione di file all'interno dell'Istituto scolastico è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.

È obbligatorio controllare i file attachements (allegati) di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

Inoltre, è severamente vietato inviare messaggi, con allegati file con contenuti inerenti alle attività dell'Istituto scolastico, contenenti eventualmente anche categorie particolari di dati (c.d. "sensibili") o giudiziari, a destinatari che non sono in relazione con l'Istituto scolastico, soprattutto se non vi è una norma di legge o regolamento che preveda tale forma di comunicazione (art. 2-ter del D.Lgs. 196/2003).

È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve informare tempestivamente il Responsabile dei Sistemi Informatici. Non si devono in alcun caso attivare gli allegati di tali messaggi.

5.1. Linee guida generali per l'utilizzo della posta elettronica

Ogni dipendente o utente, in caso di assenza per qualsiasi motivo (ferie, allontanamento temporaneo dal posto di lavoro, malattia) e al fine di non interrompere né rallentare i processi produttivi e/o lavorativi, ha la facoltà di inserire nel proprio account di posta elettronica la funzione di risposta automatica, contenente eventualmente le coordinate di altri colleghi a cui rivolgersi in sua sostituzione; il delegato (o fiduciario) potrà in questo modo ricevere i messaggi di posta elettronica del dipendente o utente assente e a lui indirizzati.

In caso di assenza prolungata dell'incaricato dall'Istituto scolastico, anche per il tramite di un soggetto all'uopo nominato (es. amministratori di sistema), potrà accedere all'account di posta elettronica istituzionale, al fine di verificare il contenuto di messaggi e utilizzare – selezionandoli - quelli utili per il regolare svolgimento dell'attività lavorativa.

In conformità delle disposizioni di legge e nel pieno rispetto del principio di non eccedenza, l'Istituto scolastico si riserva la facoltà di effettuare controlli circa le modalità e le finalità di utilizzo della posta elettronica, soprattutto al fine di verificare la funzionalità e la sicurezza del sistema informatico. Ciò avverrà avvalendosi della facoltà di effettuare i c.d. "controlli difensivi", che saranno effettuati saltuariamente e/o a campione e solo in caso di stretta necessità, sull'intera area del traffico dati della posta elettronica dell'Istituto scolastico ed esclusivamente per finalità di difesa e tutela del patrimonio e della sicurezza dell'Istituto scolastico.

Salvo quanto indicato, in nessun caso verrà effettuato l'accesso diretto alla casella di posta elettronica dei dipendenti, se non in seguito a gravi e comprovati motivi che possano rilevare il compimento di reati o condotte illecite oppure su segnalazione dell'Autorità Giudiziaria nell'ambito di indagini svolte per la repressione, accertamento e prevenzione di reati. Le attività di verifica verranno svolte esclusivamente dal Responsabile dei Sistemi Informativi.

Si fa presente, inoltre, che l'Istituto scolastico, nel caso di dipendenti che abbiano cessato il loro rapporto di lavoro per qualsiasi causa presso l'Istituto scolastico (Titolare del trattamento), attiverà un messaggio automatico sull'account del dipendente cessato che segnali al mittente il reindirizzamento dell'e-mail ad altro dipendente

(seguirà dopo un periodo non superiore a 6 mesi la disattivazione dell'account). Si fa presente, inoltre, che l'Istituto scolastico potrà, in casi eccezionali, accedere alla posta elettronica del dipendente o dell'utente che abbia cessato il suo rapporto di lavoro per qualsiasi causa (dimissioni, licenziamento, etc.) e ciò in quanto trattasi di uno strumento del datore di lavoro messo a disposizione del dipendente, oltre che necessario per garantire la continuità dell'attività lavorativa dell'organizzazione e del dipendente subentrante.

Tutti i messaggi di posta elettronica (inviati e ricevuti), i cui contenuti possono avere una rilevanza giuridica e commerciale per l'Istituto scolastico, costituiscono corrispondenza istituzionale (disciplinata dalle norme del Codice Civile e, in particolare, in base al combinato disposto degli articoli 2214 e 2220) e pertanto saranno conservati in base ai piano di conservazione e scarto d'archivio dell'Istituto scolastico. In ogni caso, il tempo di conservazione dei messaggi di posta elettronica non sarà superiore a quello necessario agli scopi che si intendono perseguire, nel rispetto dei principi di finalità, pertinenza e non eccedenza, nonché di limitazione della conservazione ai sensi del Regolamento UE 2016/679.

6. Utilizzo dei supporti removibili

E' richiesta particolare attenzione nell'utilizzo di supporti removibili (chiavette USB, memory stick, HD esterni), evitando di memorizzarvi informazioni per periodi superiori a quelli strettamente necessari.

Tutti questi strumenti devono essere conservati con cura, evitando di lasciarli incustoditi, e alla fine della giornata lavorativa è richiesto di depositare tali strumenti in un armadio chiuso e/o nella propria cassettiera.

L'Istituto scolastico fornisce ove necessario i supporti removibili necessari per la normale attività lavorativa; è fatto divieto di utilizzare device personali.

Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …), se non con l'autorizzazione espressa del Responsabile dei Sistemi Informativi.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Responsabile dei Sistemi Informativi nel caso in cui vengano rilevati virus.

<u>Dati sensibili / Informazioni classificate come riservate</u>

Qualora vi fosse la necessità di utilizzare i supporti removibili per la temporanea conservazione di categorie particolari di dati (c.d. "dati sensibili") o di informazioni riservate è necessario rivolgersi al Responsabile dei Sistemi Informativi per la predisposizione di un sistema di crittografia dei dati.

I supporti removibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

<u>Procedure di controllo</u>

I dipendenti e i collaboratori, che hanno accesso all'utilizzo di tali supporti, sono consapevoli che l'Istituto scolastico effettua controlli finalizzati alla verifica dell'utilizzo di tali supporti.

In particolare durante gli audit interni verrà verificato il rispetto delle regole di utilizzo.

7. Documenti Digitali/Cartacei Riservati

I documenti digitali/cartacei classificati come Riservati possono essere utilizzati unicamente dal personale autorizzato per esclusive finalità lavorative. E' quindi vietato qualsiasi utilizzo degli stessi per finalità personali.

Il personale che riceve per via elettronica documenti/informazioni riservate non può in alcun caso inviarli o metterli comunque a conoscenza di personale non autorizzato.

Le informazioni/documenti riservati devono essere salvati solo nelle apposite aree all'interno dei server dell'Istituto scolastico.

Le informazioni/documenti riservati possono essere stampati solo in caso di necessità, i documenti cartacei riportanti informazioni di origine elettronica riservate devono essere distrutti nel momento in cui termini la loro funzione.

8. Documenti Digitali/Cartacei ad Uso Interno

I documenti digitali/cartacei ad uso interno possono essere utilizzati dal personale dell'Istituto scolastico per esclusive finalità lavorative, consapevole che queste costituiscono un bene da proteggere. E' quindi vietato qualsiasi utilizzo degli stessi per finalità personali. I documenti "ad uso interno" possono circolare liberamente nell'ambito dell'organizzazione ma non sono destinati alla diffusione. L'eventuale divulgazione esterna può risultare inopportuna rispetto agli interessi istituzionali. Pertanto, a tal fine è necessario richiedere un'autorizzazione al Dirigente Scolastico.

9. Formazione

La prima misura di sicurezza per la protezione delle informazioni è indubbiamente la preparazione e consapevolezza dei dipendenti e degli utenti nello svolgere il proprio lavoro in modo sicuro. Consapevolezza e preparazione sono aspetti che fanno parte del background del dipendente e dell'utente, ma che possono essere sviluppati anche attraverso specifica formazione nelle varie fasi della vita lavorativa.

In ambito sicurezza delle informazioni e Data Protection è stata pianificata una specifica attività dedicata alla formazione, mediante condivisione di materiale informativo e organizzazione di specifici corsi di aggiornamento. In questo modo si potranno reperire conoscenze, risorse e documenti per accrescere le proprie competenze e di riflesso migliorare la gestione delle informazioni dell'Istituto scolastico.

Periodicamente si procede a interventi formativi specifici per chiunque tratti dati all'interno della scuola, per renderli edotti dei rischi che incombono sui dati, delle misure da adottare per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure organizzative e tecnologiche adeguate che sono state adottate o che sono da adottare. La formazione viene programmata al momento dell'ingresso in servizio, in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

Il Responsabile della Protezione dei Dati dell'Istituto scolastico è a disposizione del dipendente e dell'utente per qualsiasi dubbio o segnalazione.

Si ricorda che i corsi di formazione previsti non sono facoltativi e che la mancata ed ingiustificata assenza può portare a provvedimenti di tipo tecnico-disciplinare.

10. Osservanza delle disposizioni in materia di Privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure organizzative e di sicurezza, come indicate nella lettera di istruzioni e autorizzazione al trattamento dei dati.

11. Non osservanza del Regolamento e Controlli

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari (individuati nel CCNL vigente) commisurati alla violazione nonché con le azioni civili e penali previste dalla normativa vigente.

L'Istituto scolastico si riserva la facoltà, nel rispetto della tutela del diritto alla riservatezza e del principio di proporzionalità e non eccedenza, di svolgere dei controlli difensivi e/o indiretti che consentano di verificare l'effettiva conformità dell'uso degli strumenti informatici alle presenti prescrizioni. I controlli possono scaturire, altresì, da alcuni presupposti quali anche l'inefficienza dell'attività lavorativa del dipendente.

La verifica circa il rispetto del presente Regolamento sarà effettuata anche attraverso gli strumenti affidati al dipendente per rendere la prestazione lavorativa e per esclusive finalità organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Istituto scolastico. Le informazioni raccolte potranno essere utilizzate dall'Istituto scolastico per tutte le finalità connesse al rapporto di lavoro e – nel caso di comportamenti contrari a quanto indicato - essere utilizzate anche per l'applicazione di eventuali provvedimenti disciplinari. Per strumenti di lavoro si intende – a titolo esemplificativo - l'utilizzo di internet, della mail, del tablet (per verifica degli accesi internet, della posta elettronica, etc.).

Pertanto, le eventuali attività di controllo e monitoraggio, al fine di prevenire utilizzi indebiti della rete o degli strumenti informatici (su pc, posta elettronica o navigazione Internet, la cui raccolta dati può avvenire anche mediante la consultazione dei file di back up), per le attività dei dipendenti e degli utenti che possono causare danni o essere fonte di responsabilità per l'Istituto scolastico, saranno svolte mediante indagine a campione e solo da soggetti a ciò preposti (es. amministratori di sistema o, eventuali soggetti esterni appositamente incaricati) e saranno comunque limitate all'area di rischio individuata (si tratta di controlli mirati e non massivi). Nessun accesso ad altri documenti (che rivestono un carattere extra lavorativo) eventualmente archiviati sul computer del lavoratore sarà effettuato da parte dell'Istituto scolastico e, relativamente alla posta elettronica, oggetto di sindacato da parte del datore di lavoro non sarà il contenuto delle comunicazioni (navigazione o posta elettronica) ma soltanto il carattere personale delle mail inviate nell'orario di lavoro o della navigazione su siti non pertinenti.

Detti controlli saranno preliminarmente compiuti solo su dati aggregati, riferiti all'intera struttura organizzativa o suddivisa per unità operative. A seguito di detto controllo anonimo, potrà essere emesso un avviso generalizzato (mediante specifica comunicazione) di rilevazione di eventuali anomalie nell'utilizzo dei presidi tecnologici, con l'invito ad attenersi scrupolosamente a compiti assegnati e alle istruzioni impartite. Se a detta comunicazione non dovessero seguire ulteriori anomalie, l'Istituto scolastico non procederà a ulteriori controlli su base individuale e non saranno comunque ammessi controlli prolungati, costanti o indiscriminati. In caso contrario, verranno inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni e, a seconda della gravità della violazione perpetrata, la sanzione prevista potrà prevedere o un semplice richiamo verbale o il divieto temporaneo o permanente dell'utilizzo di strumenti informatici, sino ad

arrivare, nei casi più gravi, alla risoluzione del rapporto di lavoro o del contratto. In ogni caso, prima di assumere qualsiasi decisione disciplinare nei confronti del lavoratore, l'Istituto scolastico inviterà il dipendente/utente a motivare la ragione dell'utilizzo degli strumenti istituzionali (es. della mail o di internet) per fini personali o contrari al presente regolamento.

I dipendenti e gli utenti, qualora venissero a conoscenza di violazioni da parte dei colleghi ai comportamenti di cui ai punti precedenti, hanno l'obbligo di denunciare immediatamente l'accaduto al Dirigente Scolastico e al Responsabile della Protezione dei Dati.

Istituto Comprensivo "R. De Simone"

1) Elenco delle condotte illecite vietate e assoggettabili a sanzione disciplinare, anche negli estremi del licenziamento, e legalmente perseguibili:

a) Navigazione intenzionale all'interno di siti web pornografici o pedo-pornografici, detenzione di file di tale natura e/o loro scambio con soggetti terzi (Licenziamento);
b) Utilizzo intenzionale della rete dell'Istituto scolastico ai fini di:
   - creare o trasmettere qualunque immagine, dato o altro materiale offensivo, diffamatorio, osceno, indecente, o che attenti alla dignità umana, specialmente se riguardante il sesso, la razza o il credo;
   - danneggiare, distruggere, cercare di accedere senza autorizzazione ai dati o violare la riservatezza di altri utenti, compresa l'intercettazione o la diffusione di parole di accesso (password) e ogni altro "dato personale" come definito dalle leggi sulla protezione della privacy (Licenziamento);
   - effettuare di qualsiasi tipo di attività volta a raggirare o compromettere i meccanismi di protezione dei sistemi informativi;
   - sfruttare qualsiasi vulnerabilità derivante da difetti di configurazione o difetti intrinseci ai programmi e/o ai sistemi al fine di commettere azioni illecite o non autorizzate (Licenziamento);
   - falsificare la propria identità (Licenziamento);
   - svolgere sulla Rete ogni altra attività vietata dalla Legge dello Stato e dalla normativa Internazionale.
c) Download intenzionale da internet di file non correlati all'attività lavorativa e per i quali derivi un danno in capo all'Istituto scolastico, di natura civile e/o penale, quale conseguenza della violazione degli obblighi imposti dal d.lgs. 29 dicembre 1992, n. 518, sulla tutela giuridica del *software* e/o dalla l. 18 agosto 2000, n. 248, contenente nuove norme di tutela del diritto d'autore (a titolo esemplificativo: file musicali, film o altro materiale coperto da diritti d'autore);
d) Accesso reiterato e per periodi di tempo complessivamente rilevanti a siti internet di contenuto non attinente all'attività lavorativa, anche dopo avere ricevuto specifici richiami in materia (Licenziamento);
e) Comunicazione della password a terzi, senza a ciò essere stati preventivamente autorizzati, nell'ipotesi che da tale comunicazione derivi un danno alla scuola.

2) Elenco delle tipologie di siti web correlati all'attività lavorativa e liberamente navigabili:

- Siti di Enti Pubblici, Ministeri o Associazioni in genere;
- Siti regionali o di aziende ad essa collegate.

Si rende noto che il Titolare del trattamento, mediante le funzioni interne preposte, provvederà a denunciare alle autorità competenti tutti i casi di utilizzo dei servizi informativi dell'Istituto scolastico ritenuti in contrasto con la normativa vigente.

L'Istituto scolastico, nella persona del Dirigente, ha facoltà di promuovere azione di rivalsa per danni provocati dall'inosservanza del Regolamento o per danneggiamento delle apparecchiature informatiche.

L'utente/dipendente e ogni destinatario del Regolamento è sempre direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet. La responsabilità si estende anche alla violazione degli accessi protetti, del copyright e delle licenze d'uso.

La violazione del presente Regolamento dell'Istituto scolastico comporta l'applicazione dei provvedimenti sanzionatori nello stesso descritti o la sospensione d'ufficio dell'utilizzo delle risorse informatiche a disposizione, fatte salve le più gravi sanzioni previste dalle norme di legge e inoltre per il personale dipendente risultano applicabili gli articoli del CCNL applicabile al rapporto in essere e l'articolo 7 dello Statuto dei Lavoratori.