Ministero dell'Istruzione e del Merito
ISTITUTO COMPRENSIVO "SANDRO PERTINI"
Via Thomas Mann, 8-20162 Milano 0288447715 - 0288447722
email: MIIC8DF00R@ISTRUZIONE.IT – PEC MIIC8DF00R@PEC.ISTRUZIONE.it
Cod.mecc. MIIC8DF00R C.F. 80124890155 Cod. Univoco Ufficio **UFTUDP**

Disposizioni operative per l'utilizzo di internet, della posta elettronica e delle risorse informatiche e telematiche dell'Istituto, in ottemperanza al Provv. del Garante per la protezione dei dati personali del 1 marzo 2007 e GDPR – Regolamento UE 2016/679

1. Obiettivo del presente documento

Obiettivo del presente documento è assicurare che l'utilizzo di internet, della posta elettronica e più in generale delle risorse informatiche e telematiche dell'Istituto avvenga in conformità a quanto prescritto dal Provvedimento del Garante per la protezione dei dati personali del 1marzo 2007, nonché in conformità a quanto prescritto dal nuovo Regolamento Europeo GDPR – Regolamento UE 2016/679.

Più in generale, il presente documento contiene una serie di norme e disposizioni di carattere operativo, finalizzate ad assicurare che l'utilizzo delle risorse informatiche e telematiche dell'Istituto avvenga in modo corretto, sicuro, efficiente ed efficace e senza aggravio di costi per l'Ente.

Si è infatti visto che le tecnologie informatiche e delle telecomunicazioni rivestono un ruolo sempre più importante sia nelle aziende che nella Pubblica Amministrazione, e possono rappresentare un fattore critico di successo per il raggiungimento e il mantenimento di parametri di efficienza, efficacia, eccellenza e qualità. Oltre a questo, un corretto utilizzo degli strumenti informatici può permettere di lavorare in maniera più sicura, piacevole e produttiva, riducendo il tempo dedicato ad attività routinarie e ripetitive, permettendo di concentrarsi su attività a più elevato valore aggiunto.

Con il progredire dell'informatica e di Internet, e più in generale all'aumentare della complessità degli strumenti, assieme ai vantaggi sopra evidenziati (efficienza, efficacia, semplificazione, etc.) hanno cominciato a presentarsi e diffondersi (e questo si può in parte considerare come il rovescio della medaglia) fattori e situazioni di criticità e di rischio, come ad esempio i virus informatici, gli "hacker", l'intercettazione e la perdita di confidenzialità delle informazioni, etc. Per questo motivo è importante che l'utilizzo degli strumenti avvenga in maniera, oltre che efficiente ed efficace, sicura, in modo da eliminare o minimizzare i fattori di rischio appena accennati.

2. Norme di carattere generale

Tutti gli strumenti e le risorse (personal computer, apparati vari, tra cui penne USB, posta elettronica, accesso ad Internet, accesso alla rete, etc.) sono di proprietà dell'Istituto, pertanto ne deve essere fatto un utilizzo a fini esclusivamente lavorativi, coerente e motivato dagli specifici compiti affidati e dal ruolo ricoperto. Deve essere evitato qualsiasi utilizzo personale oppure non chiaramente riconducibile al proprio ruolo e alle proprie mansioni lavorative. **Sono di proprietà dell'Istituto tutte le mail in ingresso ed in uscita, nonché tutti i files memorizzati su hard disk, su server di rete, e più in generale su qualsiasi supporto di memorizzazione. In caso di cessazione o interruzione, anche temporanea, del rapporto di lavoro, è fatto tassativo divieto al dipendente o collaboratore di cancellare qualsiasi messaggio di posta elettronica, sia in ingresso che in uscita, e qualsiasi tipo di file o informazione, anche su supporto cartaceo.**

L'Istituto potrà verificare o far verificare da soggetti incaricati lo stato di utilizzo e accedere al contenuto degli strumenti e delle risorse concesse in uso (compresi personal computer, anche portatili, hard disk, cartelle di rete, posta elettronica, siti internet visitati, etc.), per verificarne il corretto ed efficiente utilizzo e per verificare che l'utilizzo avvenga in ottemperanza alle presenti disposizioni operative e per fini strettamente lavorativi.

L'utilizzo degli strumenti e delle risorse deve essere improntato a criteri di sicurezza, efficienza, efficacia ed economicità, evitando sprechi ed evitando di causare attività non necessarie a carico dell'Istituto.

In caso di dubbio, oppure in caso di poca chiarezza o insufficienza delle istruzioni ricevute, bisogna astenersi dall'intraprendere azioni in autonomia, che anche in buona fede potrebbero comportare danni, disservizi o malfunzionamenti, ed è invece necessario chiedere istruzioni al Dirigente Scolastico o al DSGA.

3. Utilizzo del Personal computer e degli apparati collegati

Il personal computer (per brevità "PC") affidato al dipendente o collaboratore è uno strumento di lavoro di proprietà dell'Istituto, temporaneamente affidato in uso al dipendente o collaboratore, che ne deve fare un uso esclusivamente per finalità lavorative e non personali e ne deve assicurare la diligente e scrupolosa custodia. Oltre al personal computer, sono soggetti alle prescrizioni di cui sopra anche apparati tipo hard disk esterni, penne USB, e in generale tutti gli apparati utilizzati unitamente al PC. Particolare cura deve essere posta nell'evitare furti o smarrimenti di supporti mobili di memorizzazione, come ad esempio hard disk esterni, chiavette USB, cd-rom, dvd, etc.

Il PC e qualsiasi programma applicativo deve essere sempre protetto da password iniziale di accesso, lunga almeno otto caratteri e modificata autonomamente da parte dell'utente finale (assegnatario del PC) ogni sei mesi e in ogni caso (certezza o anche semplice sospetto) in cui la password abbia perso la segretezza. L'accesso iniziale deve avvenire esclusivamente con la propria user-id (e ovviamente con la relativa password), assegnata dall'Istituto all'utente. Non è permesso accedere con altre user-id, differenti da quella assegnata.

Il PC deve esser essere protetto da bloccaschermo con password, che deve attivarsi automaticamente dopo al massimo dieci minuti o meno di inattività, oppure tramite combinazione di tasti <simbolo di Windows> - L attivata volontariamente dall'utente prima di allontanarsi dal PC.

Alla fine dell'attività lavorativa il PC deve essere spento, ed è necessario attendere e constatare l'effettivo regolare spegnimento. Questo punto è molto importante, poiché talvolta per vari motivi viene visualizzato un messaggio di errore e di anomalia che attende un ok o una scelta da parte dell'utente, che interrompe il processo di spegnimento. In questo caso chiunque si trovi a passare nelle vicinanze successivamente potrebbe accedere al computer e al suo contenuto , compiendo operazioni potenzialmente dannose o non consentite.

Le configurazioni hardware e software del PC non devono essere per nessun motivo modificate. In caso di effettiva necessità, deve esserne fatta richiesta al Dirigente Scolastico o al DSGA. In particolare non è consentito installare o disinstallare autonomamente periferiche o apparati, e non è consentita l'installazione o la disinstallazione autonoma di programmi.

E' esplicitamente vietato installare o usare programmi di accesso o controllo remoto, o che permettano comunque di intercettare le comunicazioni di altri utenti o di accedere ai PC degli altri utenti. La non ottemperanza può integrare uno o più dei seguenti reati o illeciti:

accesso abusivo ad un sistema informatico o telematico (art. 615ter C.P.)

violazione, sottrazione e soppressione di corrispondenza (art. 616 C.P.)

intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617quater C.P.)

installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche.

4. Utilizzo della rete locale (LAN)

La rete locale (chiamata anche "LAN" – Local Area Network) è un mezzo che permette di condividere risorse, come ad esempio aree di memorizzazione su server, stampanti, plotter, altri PC, etc.

In linea generale, tranne eccezioni ben individuate e motivate, tutti i documenti (quindi non solo quelli "ufficiali", ma anche quelli di lavoro o le bozze) devono essere memorizzati esclusivamente nelle cartelle di rete su server, e non in locale sul proprio PC. In questo modo ne viene assicurato il regolare salvataggio, e quindi la possibilità di ripristino in caso di necessità; viene inoltre assicurato che i documenti saranno accessibili solo ai soggetti o agli uffici autorizzati, con i corretti permessi di accesso (es. sola lettura, controllo completo, etc.), nonché la necessaria protezione antivirus.

Nel caso vi siano stampanti di rete collocate in aree distanti, è necessario porre particolare attenzione al fatto che le stampe potrebbero essere generate in aree o in contesti accessibili al pubblico o a soggetti – anche interni – non autorizzati; quindi è necessario ritirare prontamente le stampe dal vassoio di stampa.

Nel caso vi siano errori o interruzioni delle stampe fatte in rete, talvolta può convenire cancellare la stampa, in quanto la ripresa o la riattivazione della stampante potrebbe avvenire successivamente, anche il giorno dopo, in momenti di non presenza del diretto interessato (l'utente che ha lanciato la stampa) e quindi i documento potrebbero essere visti o raccolti da personale estraneo o non autorizzato o titolato; quanto appena detto è particolarmente importante e significativo nel caso di documenti con contenuto riservati o confidenziali (es. documenti riguardanti i dipendenti o gli alunni) o contenenti dati sensibili o giudiziari o comunque riservati.

E' vietato collegare alla rete PC, PC portatili, stampanti, plotter e qualsiasi tipo di apparato, poiché potrebbe compromettere la sicurezza e l'operatività della rete e delle risorse ad essa collegate. In caso di necessità il collegamento deve essere richiesto ed autorizzato dal Dirigente Scolastico.

5. Utilizzo della posta elettronica

La casella di posta elettronica è uno strumento di lavoro di proprietà dell'Istituto, temporaneamente affidata in uso al dipendente o a un gruppo di dipendenti, pertanto in linea di principio, come tutte le altre risorse, deve essere utilizzata solo per lavoro e non per scopi personali.

La persona assegnataria della casella di posta elettronica è responsabile del suo corretto utilizzo.

E' vietato utilizzare qualsiasi indirizzo di posta elettronica con dominio internet riconducibile all'Istituto per iscriversi o partecipare a forum, gruppi di discussione, mailing list, etc. se non nei casi autorizzati per iscritto dal Dirigente Scolastico, per esigenze lavorative. E' vietato inoltre rispondere o comunque partecipare alle c.d. "catene di S. Antonio", soprattutto nei casi che descrivano situazioni di bisogno o "commoventi". E' vietato inoltre utilizzare la posta elettronica per inviare comunicazioni del tipo "è nato il figlio di…", "invito alla cena …", "si sposa … raccogliamo soldi per il regalo", etc.

E' vietato rispondere ai messaggi di "spam", e a tutti i messaggi di origine ignota o dubbia, che richiedano di rispondere al messaggio di posta elettronica inviato o di confermarne la correttezza. Si ricorda che il sistema antispam è "euristico", quindi non infallibile, per cui potrebbero venire bloccate alcune mail (i cosiddetti "falsi positivi") che in realtà non sono spam. In questo caso L'Istituto è sollevato da qualsiasi responsabilità.

E' necessario porre particolare attenzione prima di aprire messaggi di provenienza dubbia o inattesa, in quanto potrebbero contenere virus o codici maligni; in particolare non bisogna aprire allegati con suffisso .EXE o .BAT, e quelli con un doppio suffisso (es. .VBS.BAT) perché molto probabilmente contengono virus. In questi casi bisogna avvertire il Dirigente Scolastico che attiverà i controlli necessari. Si ricorda comunque che – sebbene più raramente – anche messaggi di posta elettronica provenienti da indirizzi conosciuti possono contenere virus.

6. Utilizzo di Internet

Come le altre risorse, il collegamento ad Internet deve essere utilizzato esclusivamente per finalità lavorative e non personali; in particolare è vietato scaricare musica, film e qualsiasi contenuto che sia coperto da diritto d'autore; parimenti è vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi esplicitamente autorizzati dal Dirigente Scolastico indispensabili per lo svolgimento delle mansioni assegnate (es. remote banking per la disposizione di bonifici).

E' vietato scaricare e/o installare programmi di qualsiasi tipo (a pagamento, freeware, shareware, etc.) se non nei casi autorizzati dal Dirigente Scolastico.

E' esplicitamente vietato visitare siti internet a contenuto erotico, pedo-pornografico, violento, razzista. E' altresì vietato visitare siti di "hacker", in quanto in questo caso vi è una forte probabilità che il computer venga infettato da virus e codici maligni, oppure diventi vittima di programmi di tipo "trojan horse", che potrebbero causare gravi disservizi al PC, alla rete, e agli altri PC in rete.

E' vietata la partecipazione a forum non professionali e a bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

L'Istituto potrà applicare per singoli e gruppi di utenti politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate con il Titolare, al fine di ottimizzare l'uso delle risorse e le prestazioni delle connessioni esistenti, tenendo conto delle esigenze delle varie tipologie di utenti.

L'Istituto potrà effettuare alcuni controlli sui siti internet visitati, sui tempi e sulle modalità di collegamento, al fine di individuare eventuali abusi e verificare l'ottemperanza alle presenti disposizioni operative. Gli eventuali controlli saranno comunque effettuati in modo non sistematico, in ottemperanza ai principi di necessità, non eccedenza e

proporzionalità e in ogni caso in ottemperanza a quanto prescritto dal Provvedimento del Garante per la protezione dei dati personali dedicato all'utilizzo di internet e della posta elettronica.

7. Utilizzo delle risorse telefoniche

Come le altre risorse, anche il telefono, il fax e più in generale tutti gli apparati di telecomunicazione devono essere utilizzati per finalità lavorative e non personali, secondo principi di efficienza ed economicità dell'utilizzo delle risorse.

Nel caso siano disponibili differenti modalità di comunicazione, deve essere utilizzata la modalità più conveniente, tenendo conto anche dei costi collegati.

Per verificare l'ottemperanza al presente regolamento, L'Istituto potrà tenere traccia delle chiamate effettuate o ricevute da ciascun dipendente, incluso l'orario di chiamata, la durata della conversazione, la numerazione chiamata o chiamante ed il contenuto della comunicazione.

Nel caso di telefonate anomale (es. eccessivamente lunghe o frequenti), il dipendente è tenuto a fornire indicazioni relativamente alla motivazione della chiamata e/o alle generalità del soggetto chiamante o chiamato.

In caso di telefonate particolarmente anomale (per durata e/o frequenza) L'Istituto potrà accedere a campione al contenuto delle chiamate e più in generale delle comunicazioni effettuate o ricevute.

8. Gestione delle password

La password, unitamente alla relativa user-id, costituisce la c.d. coppia di "credenziali di autenticazione", necessarie per accedere a qualsiasi risorsa (PC, programma applicativo, registro elettronico, rete, file, etc.) che debba essere protetta. La user-id è fissa e individua univocamente l'utente assegnatario, come una sorta di "codice fiscale", mentre la password può e deve essere modificata dall'utente periodicamente.

Le password devono essere tenute segrete e non devono essere comunicate ad altre persone per nessun motivo; nel caso sia necessario condividere un documento o una risorsa con un collega, non si deve comunicare la propria password al collega, ma si devono utilizzare a livello di rete dei meccanismi corretti di condivisione che potranno venire messi in atto facendone richiesta al Dirigente Scolastico**. Il rivelare la propria password ad altri costituisce reato di comunicazione o diffusione abusiva di codici di accesso a sistemi informatici o telematici, punibile ai sensi dell'art. 615quater del Codice Penale con la reclusione da uno a due anni e con la sanzione amministrativa da Euro 5.164 a Euro 10.329.**

La password (e più in generale le password) devono essere modificate ogni sei mesi , e ogni tre mesi nel caso di documenti contenenti dati sensibili o giudiziari. La password deve inoltre essere modificata ogniqualvolta abbia perso la sua segretezza o ve ne sia il sospetto. La mancata modifica delle password con le frequenze richieste costituisce reato di omessa adozione di misure minime di sicurezza, punibile ai sensi dell'art. 169 del D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali) con la reclusione sino a due anni o con la sanzione amministrativa da Euro 10.000 a Euro 50.000.

All'atto della modifica, la nuova password deve essere scritta e posta all'interno di una busta chiusa e sigillata, datata e firmata sul lato esterno, e consegnata al soggetto incaricato della custodia delle password.

Per facilitare le operazioni di modifica, è possibile mettere in atto meccanismi automatici che all'approssimarsi della data di scadenza della password producano dei promemoria e ad un certo punto "costringano" l'utente finale a modificare la password.

Le password devono essere lunghe almeno otto caratteri e non contenere riferimenti agevolmente riconducibili (es. nome) all'utente. Si rammenta che l'utilizzare come password parole di senso compiuto aumenta significativamente i rischi che la password possa venire "indovinata" o scoperta da programmi di "forzatura" delle password, per cui si consiglia di non utilizzare parole di senso compiuto, o almeno di inserire una cifra in qualsiasi posizione.

9. Utilizzo dei supporti di memorizzazione

E' necessario porre particolare attenzione ai supporti mobili di memorizzazione (floppy-disk, hard-disk esterni e interni, cd-rom, chiavette USB, etc.) perché il rischio di perdita, asportazione, furto, accesso da parte di non autorizzati, etc. è molto elevato. Quanto detto vale in particolar modo per le chiavette USB, che sono molto piccole e possono contenere quantità elevatissime di dati. Pertanto questo tipo di risorse deve essere custodito con diligenza e scrupolo.

Le chiavette USB non devono essere mai utilizzate come supporto unico o principale di memorizzazione, ma solo per fare eventuali copie temporanee. I documenti devono sempre e comunque venire memorizzati in via prioritaria sul server di rete.

Nel caso di utilizzo di chiavette USB, prima di scollegarle del PC devono essere disattivate; se non viene effettuata la disattivazione vi è il forte rischio che tutti i dati contenuti nella chiavetta USB vadano perduti.

Bisogna porre particolare attenzione ai supporti contenenti informazioni confidenziali o riservate, o dati personali o sensibili: in questo caso, quando i dati non sono più necessari, la cancellazione deve avvenire con modalità che non permettano il successivo recupero. Se trattasi di supporti non riscrivibili, come ad esempio cd-rom, bisogna rendere il supporto inutilizzabile mediante frattura fisica dello stesso.

I supporti magnetici contenenti dati sensibili o giudiziari devono essere custoditi in archivi o contenitori chiusi a chiave o comunque con modalità tali da assicurare la riservatezza dei dati ed evitare che vi sia accesso e conoscenza da parte di soggetti non autorizzati.

10. Protezione antivirus

Ciascun utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informativo provocato da virus o da altro software o codice maligno.

E' necessario verificare il regolare funzionamento del software antivirus installato, e segnalare immediatamente al Dirigente Scolastico i casi in cui l'antivirus sia stato disinstallato o non sia funzionante.

Nel caso il software antivirus rilevi la presenza di un virus**, bisogna immediatamente** sospendere ogni elaborazione senza spegnere il computer e segnalare l'accaduto al Dirigente Scolastico o al DSGA.

Non è consentito l'utilizzo di supporti di memorizzazione (es. chiavette USB, cd rom, hard disk esterni etc.) di provenienza ignota. Ogni dispositivo di memorizzazione di provenienza esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, si dovrà avvertire immediatamente il Dirigente Scolastico o il DSGA.

Soggetti preposti alla verifica della corretta applicazione e dell'ottemperanza al presente regolamento

La responsabilità di vigilare sulla corretta applicazione e sull'ottemperanza alle presenti disposizioni operative è affidata al Responsabile della protezione dei dati designato ai sensi dell'art. 37 del GDPR e al Dirigente Scolastico.

La verifica dell'ottemperanza alle presenti disposizioni operative potrà venire effettuata anche con controlli e ispezioni a campione o su segnalazione o richiesta del Dirigente Scolastico o del DSGA.