MINISTERO DELL'ISTRUZIONE E DEL MERITO
Ufficio Scolastico Regionale per il Lazio
ISTITUTO COMPRENSIVO 2 ALATRI "SACCHETTI SASSETTI"
Sede legale in Via Madonna Della Sanità 5/A 03011 Alatri (FR)
Tel. 0775434030 - Cod. Fisc.: 80010450601 - Cod. Mecc.: FRIC83800G
Email: fric83800g@istruzione.it – PEC: fric83800g@pec.istruzione.it

PRIVACY POLICY

per l'utilizzo degli strumenti di lavoro adottato dall'Istituto Scolastico

INDICE

1. PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, Tablet, Smartphone e più in generale ogni apparato in grado di connettersi alla rete, espone l'Istituto e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legislazione sul diritto d'autore e sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Istituto stessa.
Premesso quindi che l'utilizzo degli strumenti di lavoro, nei quali sono compresi anche i sistemi e le risorse informatiche e telematiche, deve sempre ispirarsi al principio della diligenza e correttezza, propri del rapporto di lavoro, l'Istituto Scolastico adotta la presente Privacy Policy diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati nonché originare responsabilità in capo all'Istituto ovvero ai singoli dipendenti.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni fornite a tutti i Soggetti Autorizzati in attuazione del Regolamento 2016/679/UE (nel seguito "GDPR") e del D.lgs. 30 giugno 2003 n. 196 (di seguito "Codice") come armonizzato dal D.lgs. 101/2018, nonché integrano le informazioni fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse. Si tiene conto, delle principali prescrizioni e le linee guida del Garante privacy in relazione al trattamento di dati personali effettuato dai datori di lavoro, (provvedimento "Linee-guida per il trattamento di dati dei dipendenti" del 23 novembre 2006) ai fini delle verifiche per il corretto utilizzo della posta elettronica e della rete Internet da parte dei dipendenti (provvedimento del 1° marzo 2007) nonché delle previsioni di all'art. 4 L. 300/70, come modificato dal D.lgs. 151/2015 relativamente ai controlli sugli "strumenti di lavoro", e tenendo presente le indicazioni fornite dal WP 29 con la "Opinion 2/2017 on data processing at work".

Dal contesto tracciato dall'Autorità Garante per la protezione dei dati personali, nelle premesse dei citati provvedimenti emerge che:

i. compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;

ii. spetta sempre ai datori di lavoro adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e dei dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità;

iii. è necessario tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;

iv. l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di file di log, della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta dei file di log di traffico e-mail e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;

v. le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili.

Alla luce delle premesse sopra riportate ed avendo in considerazione che l'Istituto nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer desk-top e/o portatili, telefoni cellulari, etc.), sono state inserite in questo documento le opportune indicazioni ed istruzioni relative alle modalità ed ai doveri che ciascun lavoratore deve osservare nell'utilizzo di tale strumentazione.

2. ENTRATA IN VIGORE DEL REGOLAMENTO E PUBBLICITÀ

2.1 Con l'entrata in vigore del presente Privacy Policy tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

2.2 Copia di questo documento viene pubblicato rilasciato al dipendente ed allegato alla comunicazione che ne ufficializza l'adozione nelle forme e con le modalità in uso presso l'Istituto Scolastico.

3. CAMPO DI APPLICAZIONE

3.1 La Privacy Policy si applica a tutti i lavoratori, ossia ai dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori/dipendenti dell'Istituto a prescindere dal rapporto contrattuale con la stessa intrattenuto.

3.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni lavoratore in possesso di specifiche credenziali di autenticazione. Tale figura sarà anche indicata quale "Soggetto Autorizzato al trattamento" nell'accezione propria dell'art. 29 del GDPR.

4. UTILIZZO DEL PERSONAL COMPUTER

4.1 **Il Personal Computer affidato all'utente è uno strumento di lavoro**.

4.2 Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer (sia esso fisso o portatile) deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

4.3 Il personal computer dato in affidamento è configurato con il proprio accesso personale user e password, le credenziali non devono, per alcun motivo essere comunicati/condivisi con altri così come per l'accesso alla rete mediante specifiche credenziali di autenticazione come meglio descritto al successivo punto 4 del presente documento.

4.4 Il personale specificamente autorizzato, al fine di garantire la sicurezza del sistema informatico, ha la facoltà, in qualunque momento, di accedere ai dati trattati da ciascuno, ivi compresi i programmi di posta elettronica, come più specificatamente precisato al successivo punto 13.1 del presente documento. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Istituto, si applica anche in caso di assenza prolungata od impedimento dell'utente. Analoghe verifiche possono essere effettuate sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. L'accesso, comunque, verrà effettuato con modalità tali da evitare qualsiasi forma di controllo. In ogni caso, l'Istituto garantisce la non effettuazione di alcun trattamento mediante sistemi *hardware* e *software* specificatamente preordinati al controllo anche a distanza, quali, a titolo esemplificativo:

- lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
- riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
- la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- l'analisi occulta di computer portatili affidati in uso.

4.5 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone lo stesso dipendente, fruitore a gravi responsabilità civili.

4.6 Si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

4.7 Salvo preventiva espressa autorizzazione del Dirigente, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi

di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, etc.).

4.8 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Dirigente o suo delegato nel caso in cui siano rilevati virus, adottando quanto previsto dal successivo punto 10 del presente Regolamento relativo alle procedure di protezione antivirus.

4.9 Il Personal Computer deve essere spento prima di lasciare la postazione di lavoro o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. 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. Al fine di evitare tali evenienze si dovrà "bloccare" l'utilizzo del PC prima di allontanarsi impostando la modalità "screen saver" che prevede la richiesta della password per riattivarne l'uso**.**

5. GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

5.1 Le credenziali di autenticazione per l'accesso al dispositivo e alla rete vengono assegnate dal Dirigente e dal suo Delegato, previa formale richiesta.

5.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), associato ad una parola chiave (password) riservata che dovrà venir custodita dal Soggetto Autorizzato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione.

5.3 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili alla persona. Per costruire la password utilizzare:

- Lettere minuscole e maiuscole, numeri e almeno un carattere tra: . ; $! @ - > <
- Non utilizzare date di nascita, nomi o cognomi propri o di parenti
- Non sceglierla uguale alla matricola o alla user-id
- Custodirla sempre in un luogo sicuro e non accessibile a terzi
- Non divulgarla a terzi e non condividerla con altri utenti

5.4 È necessario procedere alla modifica della parola chiave a cura dell'utente, ove ciò non avvenga grazie a processi automatici del sistema informativo, al primo utilizzo e, successivamente, almeno ogni sei mesi (ogni tre mesi nel caso invece di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici).

5.5 Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il Delegato.

6. UTILIZZO DELLA RETE INTERNA

6.1 Per l'accesso alla rete dell'Istituto ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

6.2 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le istruzioni impartite.

6.3 Le cartelle utenti presenti nei server dell'Istituto sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte dell'Istituto. Si ricorda che la responsabilità dei dati salvati all'interno dei dispositivi: server, pc, cloud ecc. è a carico del singolo utente.

6.4 Il Dirigente e suo Delegato possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosa per la sicurezza.

6.5 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi del proprio dispositivo/cartella, con cancellazione dei file

obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

7. UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI

7.1 Tutti i supporti magnetici rimovibili (CD e DVD riscrivibili, supporti USB, hard-disk removibili, ecc.), contenenti dati rilevanti, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto e/o smarrito.

7.2 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale preposto e seguire le istruzioni da questo impartite per una corretta cancellazione/distruzione.

7.3 In ogni caso, i supporti magnetici contenenti dati particolari/sensibili, secondo la definizione dell'art. 4 del GDPR, devono essere adeguatamente custoditi dagli utenti e risposti in armadi chiusi ad accesso controllato.

7.4 È vietato l'utilizzo di supporti rimovibili personali di ogni tipologia.

7.5 L'utente è responsabile della custodia dei supporti e dei dati personali in essi contenuti.

8. UTILIZZO DI PC PORTATILI

8.1 L'utente è responsabile dei dispositivi portatili assegnatogli, deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

8.2 Ai PC portatili si applicano le regole di utilizzo previste per il desktop di cui al punto sopra.

8.3 I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

9. USO DELLA POSTA ELETTRONICA

9.1 **La casella di posta elettronica assegnata all'utente è di proprietà dell'Istituto Scolastico e in quanto tale uno strumento di lavoro.**

9.2 Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

9.3 L'uso della e-mail d'Istituto, per quanto configurata con nome.cognome@dominioistituto.edu.it è di natura esclusivamente istituzionale e non personale, il contenuto, così come eventuali allegati, deve riguardare e riferirsi esclusivamente alle attività lavorative.

9.4 È fatto divieto di utilizzare le caselle di posta elettronica d'Istituto per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo e non esaustivo, l'utente non potrà utilizzare la posta elettronica per:

i. l'invio e/o il ricevimento di contenuti e/o documenti inerenti alla sfera personale; allegati quali filmati o brani musicali; ogni altro allegato non legati all'attività lavorativa;
ii. l'invio e/o il ricevimento di comunicazioni personali per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list, etc.;
iii. la partecipazione a catene telematiche, qualora si dovessero ricevere messaggi di questo tipo, si deve comunicarlo immediatamente al Titolare e/o al Delegato Interno al trattamento. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.
iv. l'invio e/o il ricevimento di messaggi contenenti informazioni dei propri familiari.

9.5 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili.

9.6 E' obbligatorio inserire in Cc il Dirigente Scolastico ogniqualvolta la e-mail da inviare abbia contenuti e/o allegati di rilievo commerciale e/o giuridico quali ad esempio, impegni contrattuali, indicazioni e/o informazioni specifiche e/o relative all'Istituto e/o documenti considerati riservati.

9.7 E' altresì obbligatorio, re-inviare al Dirigente Scolastico, ogni e-mail ricevuta dalle caratteristiche di cui al punto precedente.

9.8 È possibile utilizzare la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

9.9 In seguito agli interventi della Corte europea dei diritti dell'uomo, considerando le linee guida dell'Autorità Garante per la protezione dei dati personali, considerando la normativa nazionale L. 300/70 s.m.i. ed in particolare visto l'art. 4 co. 3 s.m.i., si evidenzia che la casella di posta elettronica, può essere oggetto di verifiche e monitoraggio da parte del datore di lavoro per determinate ragioni quali ad esempio, per garantire la sicurezza informatica, per rispettare le normative sulla privacy o per investigare eventuali violazioni della policy e circolari emanate ora per allora. I controlli effettuati dal personale tecnico autorizzato, in ogni caso non potranno mai essere sistematici e illimitati.

9.10 Alla cessazione del rapporto di lavoro, l'account della e-mail d'istituto del dipendente sarà disattivato, verrà predisposto un sistema automatico di risposta che segnali al mittente che l'indirizzo non è più attivo e che indichi a chi poter scrivere in alternativa. La conservazione delle e-mails sarà limitata per il periodo rilevante ai fini giuridici e/o di sicurezza e secondo le indicazioni normative e linee guida ora per allora in vigore.

9.11 Secondo i risultati di ricerca la violazione dei dati, data-breach causato dal phishing è aumentato notevolmente negli ultimi anni, è necessario porre la massima attenzione al contenuto e al tipo di allegati presenti nella mail, verificare l'identità dell'invio e della richiesta, non fornire mai informazioni personali a meno di essere sicuri dell'identità del mittente, non cliccare mai su link o download da fonti sconosciute.

10. NAVIGAZIONE IN INTERNET

10.1 **I dispositivi assegnati al singolo utente ed abilitati alla navigazione in Internet costituisce uno strumento istituzionale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa**. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

10.2 In questo senso, a titolo puramente esemplificativo, l'utente **non potrà** utilizzare Internet per:

- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web se non strettamente attinenti all'attività lavorativa;
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dal Dirigente e comunque nel rispetto delle normali procedure di acquisto nell'ambito lavorativo;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati;
- l'accesso, tramite Internet, a caselle webmail di posta elettronica personale, salvo specifica autorizzazione.

10.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Istituto può prevedere l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a specificati siti inseriti in una black list.

10.4 In conformità al punto 3.3, il personale Autorizzato potrà procedere a controlli sulla navigazione finalizzati esclusivamente a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, es. mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 6 mesi.

11. PROTEZIONE ANTIVIRUS

11.1 Tutti i sistemi informatici sono protetti da software antivirus aggiornato periodicamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico istituzionale mediante virus o mediante ogni altro software aggressivo.

11.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale preposto.

11.3 Ogni dispositivo magnetico di provenienza esterna all'Istituto dovrà essere verificato mediante il programma antivirus prima del suo utilizzo.

12. UTILIZZO DEI TELEFONI E FOTOCOPIATRICI DELL'ISTITUTO.

12.1 L'eventuale telefono affidato al lavoratore è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa se non diversamente indicato e autorizzato. Qualora assegnato un cellulare (smartphone, tablet, etc.) istituzionale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai dispositivi si applicano le seguenti regole: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa se non diversamente indicato e autorizzato.

12.2 L'uso promiscuo dei dispositivi è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dal Dirigente.

12.3 È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione.

12.4 Stampare semplicemente un documento e dimenticarsi la stampa può costituire un rischio per la riservatezza e tutela dei dati personali in esso contenuti.

13. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

13.1 È obbligatorio attenersi alle disposizioni in materia di protezione dei dati personali previste dal GDPR, e dal Codice privacy, rispettando le misure di sicurezza adottate dall'Istituto, nonché le istruzioni fornite con la designazione a "Soggetto Autorizzato al trattamento dei dati", come previsto dall'art. 29 del GDPR, applicando puntualmente le disposizioni ivi contenute nonché ogni ulteriore indicazione e comunicazione impartite dall'Istituto.

13.2 I "Soggetti Autorizzati" che sono addetti alle attività di amministrazione e gestione dei Sistemi, Data Base e della Infrastruttura di connessione dovranno rispettare le specifiche istruzioni loro fornite al fine di rispettare i principi di necessità e di legittimità e correttezza nella effettuazione delle loro attività. I nominativi di coloro che hanno competenza sui sistemi che trattano dati personali dei dipendenti dell'Istituto potranno essere comunicati nelle modalità e con le forme previste dalla normativa applicabile.

14. ACCESSO AI DATI TRATTATI DALL'UTENTE

14.1 Per motivi di sicurezza del sistema informatico e per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) comunque estranei a qualsiasi finalità di controllo del lavoratore e dell'attività lavorativa, è facoltà dell'Istituto, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici istituzionali e ai documenti ivi contenuti.

15. GESTIONE ARCHIVI CARTACEI

15.1 Quando si tratta di applicare e adottare il GDPR, per i documenti cartacei come per qualsiasi informazione personale detenuta, i soggetti autorizzati dell'Istituto devono esaminare le modalità di archiviazione delle informazioni e agire secondo le seguenti regole.

15.2 I documenti cartacei da conservare devono essere gestiti in modo da poter essere rintracciati e individuati facilmente. I documenti cartacei contenenti dati personali comuni e particolari "sensibili", vedi documentazione PEI, DSA, PCTO ecc. e/o giudiziari, devono essere conservati in armadietti chiusi a chiave il cui accesso, controllato, è limitato soltanto alle persone autorizzate a quel trattamento.

15.3 Lo smaltimento sicuro della carta deve essere una priorità, in particolare ora che l'UE ha aumentato le sue richieste in materia di protezione dei dati. I documenti cartacei non più necessari devono essere smaltiti in modo conforme. Bisogna utilizzare la macchina distruggidocumenti o in mancanza agire manualmente spezzettando i fogli in piccole parti in modo da non essere più ricomponibili.

15.4 I documenti cartacei – tutti - che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti nel periodo di intervallo meridiano e a fine giornata e non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

15.5 I documenti cartacei contenenti dati particolari sensibili o giudiziari devono essere controllati e custoditi dai soggetti autorizzati in modo che non vi possano accedere persone prive di autorizzazione. La loro consultazione deve avvenire per il tempo strettamente necessario alla necessità di utilizzo e, subito dopo, i documenti devono essere nuovamente archiviati.

15.6 La presenza di ospiti o di personale non autorizzato non è consentita in luoghi in cui siano presenti documenti cartacei in vista.

15.7 Evitare assolutamente di prendere appunti su fogli di carta accumulati per il riciclo senza badare a ciò che è stampato sul retro: tipicamente si tratta di vecchi documenti stampati che possono contenere dati personali e particolari sensibili o giudiziari.

16. 15. SISTEMI DI CONTROLLI GRADUALI

16.1 In caso di anomalie e su specifico mandato del Dirigente, il personale nominato Soggetto Autorizzato del trattamento o gli addetti alla manutenzione, Amministratori IT, effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti istituzionali e si inviteranno gli utenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere computi solo in caso di successive ulteriori anomalie.

16.2 In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

17. SANZIONI

17.1 È fatto obbligo a tutti i lavoratori di osservare le disposizioni portate a conoscenza con il presente documento. Il mancato rispetto o la violazione delle regole sopra ricordate possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice civile e sono perseguibili nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal Contratto di lavoro sottoscritto ovvero dal vigente CCNL, nonché con tutte le azioni civili e penali consentite.

18. AGGIORNAMENTO E REVISIONE

18.1 Tutti gli utenti possono proporre integrazioni e/o correzioni motivate al presente documento. Le proposte verranno esaminate dall'Istituto.

18.2 Il presente documento è soggetto a revisione con frequenza periodica anche in funzione dell'introduzione di nuovi strumenti di lavoro e/o informatici, dell'evoluzione tecnologica o di cambiamenti normativi.

18.3 Documento aggiornato in data settembre 2024.

Il Dirigente Scolastico
(Prof. Antonio Melis)

PRIVACY POLICY

per l'utilizzo degli strumenti di lavoro adottato dall'Istituto Scolastico

Il/La sottoscritto/a _____

Dichiara di aver ricevuto la privacy policy per l'utilizzo degli strumenti di lavoro.

Luogo e data _____ Firma _____