Ministero dell'Istruzione e del Merito
ISTITUTO COMPRENSIVO "A. DE CURTIS"
Scuola dell'Infanzia, Primaria e Secondaria di I Grado ad Indirizzo Musicale
Via Municipio, s.n.c. – 80036 PALMA CAMPANIA (NA) Tel. 081-8241231 Fax 081-5101507
e-mail: naic8cq00b@istruzione.it e-mail pec: naic8cq00b@pec.istruzione.it
C.F.: 84003930637 C.M.: NAIC8CQ00B
Codice Univoco Fatturazione Elettronica: *UF3ZDY*

REGOLAMENTO UTILIZZO ATTREZZATURE INFORMATICHE

La diffusione delle tecnologie informatiche nel mondo della scuola ed il progressivo passaggio della società verso modelli di comunicazione sempre più integrati ed interconnessi rendono fondamentalelo sviluppo di una cultura della sicurezza del proprio patrimonio informativo e della tutela dei diritti degli interessati.Con l'entrata in vigore delle nuove **Misure minime di sicurezza ICT per le pubbliche amministrazioni emanate da AGID e l' entrata a regime della normativa europea e nazionale (Regolamento UE 2016/679 e Codice della privacy – D.Lgs. 196/2003, modificato dal D.Lgs 101/2018)** in materia di protezione dei dati personali L'istituto I.C. ANTONIO DE CURTIS ha avviato un percorso di aggiornamento e rafforzamento delle proprie politiche di sicurezza informatica, al fine di garantire l'integrità e la disponibilità dei dati trattati, tenendo, altresì, conto delle ulteriori e specifiche normative e prescrizioni nazionali dettate in materia. È dovere, infatti, della nostra Amministrazione individuare il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione per il trattamento dei dati personali, nonché adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità.
L'elevato uso delle tecnologie informatiche (e in particolare l'accesso alla rete informatica e telematica, Internet e posta elettronica) e la messa a disposizione, da parte dell'Istituto , al proprio personale e agli studenti di strumenti informatici di ultima generazione (computer portatili, tablet, Personal Computer Fissi , Monitor Interattivi , Lavagne interattive , Videoproiettori , Multifunzioni etc.) come strumenti a supporto delle attività didattiche e amministrative ,

nell'ottica di uno svolgimento più agevole delle attività, impone la necessità di regolamentarne l'utilizzo attraverso specifiche disposizioni; ciò al fine di fornire agli utenti dei predetti sistemi informatici un'adeguata informazione circa le modalità e i doveri che ciascuno di essi deve osservare per il corretto uso di detta strumentazione, nello svolgimento dei compiti istituzionali, in modo che possano, contestualmente, collaborare alle politiche di sicurezza messe in atto.

Vige, infatti, in capo agli utilizzatori finali che svolgono, a qualsiasi titolo, attività didattiche e/o amministrative nell'Istituto Scolastico , oltre all'obbligo di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa ed idonei a non causare danni o pericoli a beni mobili ed agli strumenti ad essi affidati, anche di non utilizzare, a fini privati, materiali o attrezzature di cui dispone per fini istituzionali.

Al fine di fornire uno strumento a tutela dei diritti patrimoniali dell'Istituto Scolastico ed a garanzia della sicurezza ed integrità del proprio patrimonio informativo, anche a tutela dei diritti degli interessati è stato deciso di redigere un regolamento per il corretto utilizzo degli strumenti informatici e telematici di proprietà di questa amministrazione .

Il sottoelencato Regolamento rispetta i principi e le disposizioni normative delle Misure di Sicurezza AGID e si conforma , altresì, alle indicazioni fornite dal Garante per la protezione dei dati personali in materia di utilizzo di strumenti informatici e telematici, nonché della posta elettronica e della rete Internet.

Premessa:

Ai sensi del Regolamento UE 2016/679, i dati possono essere classificati come segue:

- **Personali:** qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Sono dati personali: nome e cognome, indirizzo, codice fiscale, foto, l'indirizzo IP o qualsiasi altra ripresa audiovisiva. La persona difatti può essere identificata anche attraverso altre notizie che non siano direttamente

identificative (ad esempio, associando la registrazione della voce di una persona alla sua immagine, oppure alle circostanze in cui la registrazione è stata effettuata: luogo, ora, situazione).

- **Categorie particolari di dati**: dati personali che, per la propria delicatezza, richiedono particolari cautele; essi sono quei dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, nonché i dati relativi alla salute o all'orientamento sessuale della persona.
- **Dati relativi a condanne penali e reati**: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (quali dati personali idonei a rilevare provvedimenti emessi dalle Autorità Giudiziarie e contenuti nel casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reati e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 c.p.p.)

Per trattamento dei dati si intende "qualunque operazione o complesso di operazioni concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati". In tale ottica è indifferente che le operazioni vengano svolte con o senza l'ausilio di mezzi elettronici, o comunque automatizzati, per cui anche i trattamenti effettuati su supporto cartaceo sono assoggettati alla normativa privacy.

Pertanto, le operazioni di trattamento si possono idealmente suddividere in tre macro-tipologie, in funzione del fatto che il loro fine sia:

a) Il reperimento delle informazioni

Tale fase è tecnicamente definita raccolta di dati, ovvero l'acquisizione delle informazioni, in qualunque modo essa avvenga: ad

esempio, direttamente dalla persona interessata, presso terzi, o mediante consultazione di elenchi o un sito web.

b) Il trattamento "interno" delle informazioni.
Si raggruppano in tale macro-tipologia le varie operazioni, poste in essere da chi raccoglie informazioni per organizzarle e renderle agevolmente usufruibili.

Esse sono:

- la registrazione dei dati, cioè il loro inserimento in supporti, automatizzati o manuali, al fine di rendere i dati disponibili per i successivi trattamenti;
- l'organizzazione dei dati in senso stretto, cioè il processo di lavorazione che ne favorisca la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione, eccetera;
- l'elaborazione, ovvero le operazioni che attribuiscono significatività ai dati in relazione allo scopo per il quale essi sono stati raccolti;
- la selezione, l'estrazione ed il raffronto, specifiche che rientrano nella ipotesi più generale della elaborazione;
- la modificazione dei dati registrati, in relazione a variazioni o a nuove acquisizioni;
- l'interconnessione, ovvero la messa in relazione di banche dati diverse e distinte tra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;
- il blocco, ovvero la conservazione dei dati con sospensione temporanea dei trattamenti;
- la conservazione dei dati, alla quale la legge dedica particolari attenzioni sotto il profilo della sicurezza;
- la cancellazione o la distruzione dei dati, anch'esse operazioni il cui compimento fa sorgere l'obbligo di effettuare taluni adempimenti.

c) L'uso delle informazioni nei rapporti con l'esterno

Sono i trattamenti più delicati, in quanto è con essi che si può concretamente ledere la sfera della riservatezza altrui: essi vengono genericamente definiti come utilizzo, ovvero la realizzazione dello scopo per cui si è provveduto alla raccolta ed ai trattamenti interni. L'utilizzo può essere:

- diretto, instaurando cioè un rapporto con la persona sul conto della quale si sono raccolte informazioni;
- indiretto, ovvero consistere nel mettere a disposizione di terzi le informazioni raccolte.

Le operazioni di utilizzo cui la legge dedica le maggiori attenzioni, in quanto si tratta di quelle potenzialmente più lesive dei diritti e delle libertà degli interessati, sono quelle con cui si mettono a disposizione di terzi i dati personali. Esse sono:

- la comunicazione, cioè il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- la diffusione, cioè il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Per lo svolgimento delle quotidiane attività lavorative, L'Istituzione Scolastica , nella persona del Dirigente Scolastico che è titolare del trattamento, necessita dell'utilizzo di apparecchiature informatiche per l'espletamento di molteplici compiti, nell'ambito di diversi ruoli e posizioni organizzative. L'uso di tali apparecchiature deve essere disciplinato da norme certe in quanto da comportamenti - anche inconsapevolmente non leciti - possono derivare conseguenze gravi, sia sul piano tecnico (come un blocco della funzionalità o una perdita di dati), sia sul piano giuridico (che possono determinare l'insorgere di responsabilità sia penali sia civili a carico, contestualmente, del titolare e del lavoratore coinvolto).

REGOLAMENTO INFORMATICO – NORME COMPORTAMENTALI

Tutto il Personale e gli alunni che utilizzano strumenti elettronici sono tenuti a prendere visione e attenersi a quanto previsto nel presente Regolamento.

- Il Personale che tratta dati personali è tenuto al rispetto di tutte le apparecchiature messe a disposizione dall'Istituto, provvedendo alla buona conservazione delle stesse, avendo cura al termine dell'orario di lavoro di lasciare la propria postazione di lavoro ordinata, efficiente e con le apparecchiature spente salvo indicazioni contrarie da parte dei responsabili (Dirigente – Dsga).
- Al momento di lasciare i locali e gli uffici, il Personale dovrà, altresì, accertarsi della chiusura delle porte e delle finestre dei locali da loro occupati.
- I personal computer ed i dispositivi mobili utilizzati dal Personale e dagli alunni sono strumenti di lavoro. Ogni utilizzo improprio può causare disservizi, costi impropri di manutenzione e, soprattutto, minacce alla sicurezza ed alla protezione dei dati personali nonchè alle informazioni costituenti patrimonio dell'amministrazione. Nei personal computer forniti è sconsigliato l'inserimento di supporti magnetici o ottici (CD-ROM, DVD-ROM, Pen Drive, etc.), se non espressamente autorizzati.
- Gli Utenti non devono modificare la configurazione del proprio personal computer; in caso di mal funzionamento dovranno richiedere l'intervento dei tecnici preposti o delle ditte esterne aventi contratti di assistenza in essere . Si fa inoltre assoluto divieto di installare sulle apparecchiature software non autorizzati. Si ricorda che il mancato rispetto delle norme relative alle licenze d'uso è perseguibile penalmente.

- E’ assolutamente vietato modificare i dati contenuti nei programmi gestionali/applicativi/piattaforme salvo quelli esplicitamente autorizzati ed è altresì vietato effettuare modifiche, attraverso gli strumenti di sviluppo, di qualsivoglia componente del programma stesso.
- Tutta la documentazione prodotta (File – Cartelle) dovrà essere inserita nelle cartelle autorizzate; periodicamente verrà effettuato un controllo dei dischi fissi al fine di verificarne l’efficienza, provvedendo all’eliminazione dei file superflui. È fatto divieto di salvare file e/o cartelle in posizioni non autorizzate.
  A tale scopo si specifica che :
  - il personale di segreteria dovrà salvare i file e le cartelle prodotte in appositi percorsi sul Server indicati dal Dirigente Scolastico o dal Dsgaallo scopo di proteggere adeguatamente i documenti , la loro integrità e di consentire la corretta esecuzione delle attività di backup degli stessi .
  - il personale docente e gli alunni dovranno salvare i file e le cartelle prodotte in appositi percorsi indicati dal Dirigente Scolastico al fine di evitare la saturazione delle risorse delle apparecchiature nonché l’integrità dei dati.
- Non è consentita la memorizzazione di documenti informatici contenenti dati personali su dischi locali del pc.
- Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
- Poiché i malware, ovvero un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al sistema su cui viene eseguito (rientrano in questa categoria virus, worm, spyware e altri programmi dannosi), costituiscono una delle minacce più frequenti alla sicurezza, è necessario che gli utenti il Personale si attengano alle seguenti norme:
  - il sistema informatico presenta software di protezione che vengono aggiornati automaticamente. Si raccomanda, pertanto, di verificare periodicamente l’effettivo funzionamento del sistema e di non disattivarli in nessuna occasione;
  - è necessario evitare il materiale che potrebbe contenere virus o altri software dannosi;
  - non scaricare mai file da mittenti sconosciuti o sospetti e, quando necessario, effettuare sempre un controllo prima di acquisire o aprire qualunque programma o documento acquisito via posta elettronica (in caso di dubbio contattare Il Dirigente Scolastico o il Dsga).

- Tutto il personale scolastico dovrà controllare che su tutti i personal computer utilizzati sia attiva una impostazione del sistema operativo che dopo un breve periodo di inattività dell’elaboratore lo blocca attivando uno screen saver protetto con password. Ciononostante, il Personale è tenuto a bloccare il proprio computer (fisso o laptop) nella pause previste o nel momento in cui debba

allontanarsi da esso per più di qualche minuto (ad esempio attivando il blocca schermo, digitando Ctrl+Alt+Canc, Blocca computer).

- L'Istituto Scolastico dispone di un server a supporto delle attività amministrative .Tutto il personale di segreteria dovrà salvare i documenti prodotti sulle apposite cartelle presenti sullo stesso al fine di consentire le attività di conservazione e backup .Gli hard disk presenti sui personal computer di segreteria e sul server nochè sul dispositivo di salvataggio dati sono crittografati come previsto dall'art.32 del Gdpr.
- Il personale dovrà salvare sempre le informazioni confidenziali sul server di rete e non all'interno dello strumento elettronico, non salvare informazioni in particolare se contengono categorie particolari di dati personali su supporti rimovibili e, nel caso vi sia la necessità di consegnare a terzi supporti rimovibili per trasferire dati accertarsi della relativa criptazione, assicurarsi che sulla chiave di memorizzazione siano presenti solamente i dati necessari da trasferire, ovvero effettuare personalmente l'operazione di trasferimento, evitando di consegnare la chiave a terzi, che potrebbero copiare le informazioni personali memorizzate;
- Eliminare sempre documenti, dischetti o altri supporti di memorizzazione in maniera sicura, evitando di gettarli nel cestino della spazzatura, senza averli previamente resi inutilizzabili e accertarsi che le informazioni non più utili vengano cancellate in modo sicuro dai supporti di dati e non conservare inutili messaggi di posta elettronica.
- I personal computer/notebook/tablet assegnati individualmente o condivisi da più utenti non devono mai essere lasciati incustoditi
- Sugli strumenti in dotazione possono essere utilizzati solamente i software forniti dall'Istituto Scolastico; pertanto, non si possono acquistare e installare software e applicazioni senza una specifica verifica e autorizzazione da parte dell'Istituzione scolastica (Dirigente/Dsga). Non installare da soli i software sul PC in dotazione, se non previa autorizzazione da parte del Dirigente Scolastico o del Dsga e non creare e non utilizzare software senza licenza d'uso (dlg. 518/92 sulla tutela giuridica del software e L. 248/2000 sulle nuove norme di tutela del diritto d'autore).
- Le unità disco (locali) sono aree di condivisione di informazioni strettamente lavorative e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia connesso all'attività lavorativa/didattica non può essere dislocato, nemmeno per brevi periodi, in queste unità è vietata, anche, la conservazione e l'archiviazione dei dati in locale sui singoli PC, salvo alcune specifiche eccezioni legate a esigenze didattiche/amministrative.
- Il Personale di segreteria si connette al Server dell'Istituzione Scolastica tramite autenticazione univoca personale. Il Personale è tenuto a non rivelare ad alcuno le credenziali di autenticazione (UserID e password) ad alcuno, colleghi, superiori amministratori di sistema inclusi, dovendo avere la massima diligenza nella custodia delle stesse e preservandone la segretezza anche durante il momento della digitazione. Qualora il Personale prenda coscienza che taluno possa aver visionato la digitazione o essere comunque a conoscenza della password, deve immediatamente provvedere cambiarla. Qualora sia richiesto di riferire in qualunque forma la password (telefonicamente,

via e-mail, ect.) il Personale è obbligato a rifiutarsi; contemporaneamente deve dare immediata comunicazione dell'accaduto al Dirigente Scolastico.

- Il Personale e gli utenti si connettono alla rete wifi dell'Istituto tramite autenticazione univoca personale. Il Personale e gli utenti sono tenuti a non rivelare ad alcuno le credenziali di autenticazione (UserID/password o Voucher) ad alcuno, colleghi, superiori amministratori di sistema inclusi, dovendo avere la massima diligenza nella custodia delle stesse e preservandone la segretezza anche durante il momento della digitazione. Qualora il Personale prenda coscienza che taluno possa aver visionato la digitazione o essere comunque a conoscenza della password, deve immediatamente provvedere cambiarla. Qualora sia richiesto di riferire in qualunque forma la password (telefonicamente, via e-mail, ect.) il Personale è obbligato a rifiutarsi; contemporaneamente deve dare immediata comunicazione dell'accaduto al Dirigente Scolastico.
- Non debbono essere utilizzate nella configurazione delle caselle di posta elettronica le opzioni di "compilazione automatica" o remember password, presenti nei browser o in altre applicazioni.
- Non debbono essere utilizzate nell'accesso alle piattaforme (tipo Mepa, Sidi,gestionale cloud, registro elettronico,e qualsiasi piattaforma cloud o web)
- le opzioni di "compilazione automatica" o remember password, presenti nei browser o in altre applicazioni.
- E' obbligatorio effettuare sempre le operazioni di logout quando si esce da una piattaforma on line (Mepa, Sidi,gestionale cloud, registro elettronico,e qualsiasi piattaforma cloud o web)
- E' obbligatorio cancellare sempre la cronologia e la cache nonché eventuali password memorizzate dal browser utilizzato per accedere a qualsiasi piattaforma prima di abbandonare la postazione di lavoro.
- È vietato comunicare, scambiare o condividere password tra più utenti (neanche se appartenenti al medesimo team di lavoro) o divulgare password personali a terzi (anche se colleghi o amministratori di sistema); la condotta non conforme a questa prescrizione può comportare sanzioni disciplinari.
- La password scelte per l'accesso alle piattaforme o al server della scuola o alla rete wifi non devono avere relazione con la propria vita privata e scolastica .
- In nessun caso devono essere annotate password in chiaro sia su supporto cartaceo sia informatico. I requisiti minimi di complessità delle password sono:
  - redazione con caratteri maiuscoli e/o minuscoli;
  - utilizzo di simboli, numeri, punteggiatura e lettere;
  - numericamente devono essere password di almeno 8 caratteri;
  - non deve trattarsi di password basate su informazioni personali, riferimenti familiari o comunque dati inerenti direttamente al soggetto titolare della password stessa.

  La password deve essere mantenuta segreta, adottando gli opportuni accorgimenti per la sua custodia.

- È vietato riutilizzare le proprie password lavorative (es. di accesso al pc, alla posta o ai vari applicativi e piattaforme) per la registrazione in altri siti web.

- Il Personale ha l'obbligo di cambiare la password di accesso agli strumenti informatici almeno ogni 45 giorni. Solo in casi eccezionali la password potrà essere resettata a cura del personale autorizzato dell'Istituzione Scolastica.
- Occorre conservare le password con diligenza per impedire che soggetti terzi ne vengano a conoscenza, segnalandone sollecitamente al Dirigente Scolastico o al Dsga l'eventuale smarrimento, sottrazione o diffusione.
- Il personale di segreteria che utilizza la Peo , salvo giustificabili eccezioni, di cui comunque risponde personalmente, non può utilizzare la posta elettronica Istituzionale per inviare, anche tramite collegamenti o allegati in qualsiasi formato (testo, fotografico, video, grafico, audio, codice, ecc.), messaggi che contengano o rimandino a:
  - i) comunicazioni commerciali private;
  - ii) materiale in violazione della Legge n. 269 del 1998;
  - iii) materiale discriminante o lesivo in relazione a razza, sesso, religione, ecc.;
  - iv) materiale che violi le normative sulla protezione dei dati personali;
  - v) contenuti o materiali che violino i diritti di proprietà di terzi;
  - vi) altri contenuti illegali.

  L'elenco riportato è da intendersi meramente esemplificativo e non esaustivo. In nessun caso il personale potrà utilizzare la posta elettronica Istituzionale per diffondere codici dannosi per i computer quali virus e simili.
- È fatto divieto di accedere, in modo non autorizzato, ad altri account, a sistemi o ad altre reti tramite operazioni di pirateria informatica, contraffazione della password o altri mezzi illeciti o fraudolenti.
- Si rende noto che per motivi organizzativi e funzionali, potrebbero essere archiviati tutti i messaggi di posta elettronica (Posta istituzionale) (anche nelle copie di back up), in uscita ed in entrata dalle caselle di posta elettronica dell'Istituzione Scolastica. Il Personale di segreteria pertanto dovrà essere consapevole dell'impossibilità di garantire la riservatezza del messaggio e dei documenti inviati e ricevuti; pertanto, sarà impegno del Personale evitare l'utilizzo delle caselle di posta elettronica per comunicazioni di carattere personale o che esulino dal contesto scolastico a cui sono preposte.
- Nei messaggi inviati tramite posta elettronica Istituzionale verrà accluso un timbro con il riferimento dell'ufficio o della persona che ha inviato l'email ,(esempio Ufficio personale 1 Ufficio didattica 2 ecc…) al fine di rintracciare l'eventuale mittente del messaggio di posta in uscita .Il Dirigente o il Dsga dovranno in qualsiasi momento poter risalire all'utente di segreteria che ha inviato la mail.
- La Posta Elettronica Certificata (detta anche PEC)dell'Istituzione Scolastica potrà essere usata solo dal Personale Autorizzato. La pec è un sistema di comunicazione simile alla posta elettronica standard ma tra indirizzi mail certificati, a cui si aggiungono caratteristiche di sicurezza e di certificazione della trasmissione tali da aggiungere

valore legale ai messaggi trasmessi. Il valore legale è assicurato dai gestori di posta PEC del mittente e del destinatario che certificano:

- data e ora dell'invio del messaggio dal parte del mittente;
- data e ora dell'avvenuta consegna del messaggio al destinatario;
- integrità del messaggio (e eventuali allegati) nella trasmissione da mittente a destinatario.
- I gestori di posta assicurano anche notifica al mittente e al destinatario di eventuali problemi occorsi durante la trasmissione.
- La PEC trasferisce sul digitale il concetto di "Raccomandata con Ricevuta di Ritorno". L'utilizzo della posta elettronica rispetto alla posta tradizionale garantisce la consegna in tempo reale.

A differenza della tradizionale posta elettronica, alla PEC è riconosciuto pieno valore legale e le ricevute possono essere usate come prove dell'invio, della ricezione ed anche del contenuto del messaggio inviato.

La comunicazione ha valore legale solo se inviata da PEC e ricevuta da PEC.

L'estensione PEC: @PEC.ISTRUZIONE.IT, dovrà accettare esclusivamente documenti provenienti da caselle di PEC,al fine di garantire gli utenti contrastando il fenomeno dello spamming e gli usi impropri.

- non è consentito l'utilizzo gli indirizzi di posta elettronica dell'Istituzione Scolastica per la partecipazione a dibattiti, Forum, newsletter o mailing list, non attinenti alla nostra amministrazione;
- non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, handicap o stato di salute o che costituiscano comunque condotta illecita.
- E' severamente vietato l'inoltro dei messaggi ricevuti sull'account di posta Dell'Istituzione Scolastica ad altro indirizzo e-mail personale se non espressamente autorizzati;
- E' severamente vietato inviare messaggi, con allegati file con contenuti inerenti alle attività dell'Istituzione Scolastica a destinatari che non sono in relazione con la stessa e/o non sono autorizzati a riceverli, salvo espressa autorizzazione scritta del Dirigente Scolastico o del Dsga.
- Il personale di segreteria è tenuto ad accedere alla casella e-mail assegnata con frequenza almeno giornaliera.
- È 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.
- La finalità dell'accesso e della navigazione su Internet è il reperimento di informazioni e di documentazione utili a supporto delle attività didattiche e amministrative; l'utilizzo dei servizi di rete per scopi non inerenti ai fini didattici e amministrativi non è consentito .
- E' fatto divieto di navigare in siti non attinenti con l'attività didattiche e amministrative , in quanto l'utilizzo al collegamento ad Internet deve essere funzionale all'attività espletata in favore dell'istituzione Scolastica. Una violazione di tale prescrizione - e qualora vengano perpetrati eventuali illeciti nella navigazione in internet - potrebbe comportare sanzioni disciplinari a carico del

contravventore attraverso le modalità e le procedure in seguito indicate al paragrafo **"Controlli indiretti"**.

- Al fine di garantire la sicurezza dei propri dati, nonché di favorire un utilizzo corretto dello strumento Internet, L'Istituto potrebbe adottare alcuni accorgimenti tecnici per prevenire illeciti da parte del Personale (è facoltà dell'Istituto, infatti, implementare delle misure preventive e delle "black list- Categorie" di siti Internet aventi l'obiettivo di impedirne la visione in quanto non ritenuti d'interesse didattico/amministrativo. Nel caso in cui un evento dannoso o una situazione di pericolo non siano stati impediti con preventivi accorgimenti tecnici, l'Istituto adotterà eventuali misure che consentano la verifica di comportamenti anomali, attraverso le modalità e le procedure indicate al paragrafo **"Controlli indiretti"**.
- L'Istituto Scolastico, al fine di prevenire determinate operazioni non consentite, ha implementato dei sistemi di filtro della navigazione che puntano a mitigare i rischi sopra esposti; 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 adotterà eventuali misure che consentano la verifica di comportamenti anomali, attraverso le modalità e le procedure di seguito specificate:
  - al fine di verificare la funzionalità, la sicurezza del sistema ed il suo corretto utilizzo, le apparecchiature di rete preposte al collegamento verso internet, memorizzano un giornale (file di log) contenente le informazioni relative ai siti che i Devices hanno visitato. Tale archivio memorizza l'indirizzo fisico delle postazioni di lavoro e non i riferimenti dell'Utente, garantendo in tal modo il suo anonimato. L'accesso a questi dati è effettuato dal Titolare del Trattamento e da persone appositamente autorizzate, nonché eventualmente da personale tecnico esterno autorizzato dall'Istituzione Scolastica;
  - l'Istituto ha attivato tali sistemi secondo le previsioni di cui al Provvedimento del Garante in materia di trattamento dati personali (Provvedimento del 1° marzo 2007), effettuando ilmonitoraggio generalizzato ed 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 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 backup per fini organizzativi o di manutenzione, per verifiche sulla funzionalità del sistema o di controllo della sicurezza dell'impianto.

In caso di accertata violazione definita tramite alert, il Dirigente Scolastico provvederà prontamente a segnalare all'interessato l'attività illecita riscontrata.
Nel rispetto al principio di finalità, pertinenza e non eccedenza, tali log vengono tenuti negli archivi dell'Istituto per 30 giorni, ossia il

tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza. L'eventuale prolungamento dei suddetti tempi di conservazione è eccezionale e può avere luogo solo in relazione all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria oppure all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità Giudiziaria.

- Al fine di evitare il grave rischio di importazione di virus informatici e di pregiudizio alla stabilità delle applicazioni dell'elaboratore, non è consentita l'autonoma installazione di programmi provenienti dall'esterno. Analogamente, non è possibile effettuare il download di file o di software aventi particolari caratteristiche dimensionali, tali da ridurre l'efficienza del sistema.
- Non è permessa la partecipazione, per motivi non didattici e/o amministrativi , a Forum, l'utilizzo di chat line, di bacheche elettroniche, mailing list o altri mezzi di comunicazione telematica non attinenti con l'attività scolastica, attuate mediante il device affidato in uso.
- È vietato collegare alla rete dati aziendale strumenti elettronici che non siano stati autorizzati dal Dirigente Scolastico o dal Dsga.
- Il Device in dotazione non deve possedere o disporre di altri collegamenti esterni diretti;
- E' vietato installare mezzi di comunicazione propri (come per esempio il modem, router , access point o qualsiasi altro apparato attivo non autorizzato dal Dirigente Scolastico e dal Dsga);
- E' vietato inviare informazioni confidenziali tramite internet o altre reti di comunicazione elettronica senza aver preso le dovute precauzioni e adottato le misure di sicurezza idonee a ridurre i rischi di accesso abusivo dei dati trasmessi.
- In generale, è opportuno non fornire indicazioni relative allo stato di salute degli utenti/personale via telefono, se non si è certi dell'identità dell'interlocutore che sta chiamando; occorre verificare comunque che l'interessato abbia autorizzato la comunicazione dei propri dati a terzi.
- E vietato utilizzare periferiche di copia /stampa(Fotocopiatrici-Stampanti ecc…) se non per scopi didattici/amministrativi.
- Non è consentito rivelare numeri telefonici interni o informazioni sull'Istituto a persone non preventivamente identificate, nonché autorizzate a conoscerle, ed è fatto divieto di lasciare documenti incustoditi presso i locali delle fotocopiatrici.
- La stampa di documentazione contenente dati personali deve avvenire ad opera di personale autorizzato a trattare tali dati; inoltre, occorre ritirare tempestivamente la documentazione dalla stampante/Multifunzione utilizzata (il riutilizzo di fogli recanti una stampa su una sola facciata, per esigenze di risparmio e di sensibilità ambientale, deve riguardare esclusivamente supporti nella disponibilità dell'autorizzato ed essere utilizzati nell'ambito delle proprie mansioni, evitando di far conoscere a terzi non autorizzati il contenuto dei documenti). I fogli contenenti dati personali non più utilizzati e per i quali non è necessaria la conservazione, prima di essere conferiti nella raccolta differenziata, devono essere trattati

in modo da renderli non intelligibili a terzi usando eventualmente un adeguato dispositivo distruggi documenti.

- ❖ Nella valutazione delle informazioni, il Personale si impegna a osservare ogni cautela perché le stesse rimangano riservate, essendo inteso che, in caso di divulgazione non autorizzata, sarà a suo carico l'onere di provare di avere adottato tali misure.
- ❖ Il Personale non può divulgare, pubblicare o comunicare in alcun modo a terzi, direttamente o indirettamente, in tutto o in parte, le informazioni apprese in occasione dello svolgimento delle mansioni, né potrà usarle, sfruttarle o disporne in proprio o tramite terzi. Tali comportamenti includono l'inoltro di mail verso l'esterno, se non per attività lavorative e vietano altresì il re-inoltro ad altri account che non siano quelli aziendali.
- ❖ Ogni Device deve essere protetto da idonei strumenti per il rischio di attività di virus informatici; lo strumento di protezione (di norma software antivirus).
- ❖ Evitare di aprire messaggi di posta elettronica provenienti da mittenti sconosciuti o sospetti e cancellarli immediatamente. In caso di dubbio contattare Il Dirigente Scolastico oppure il Dsga.
- ❖ Nel caso di utilizzo di supporti di memorizzazione esterni fermo restando quanto previsto nel presente Regolamento in merito alla possibilità di utilizzo di detti supporti, controllare sempre che i file memorizzati non siano infettati da virus attraverso la scansione del supporto.
- ❖ La documentazione cartacea viene spesso sottovalutata rispetto ai file presenti sui propri Devices. La riduzione del numero di fogli stampati rappresenta un grande obiettivo dal punto di vista della salvaguardia delle risorse naturali, ma anche un ottimo sistema per proteggere l'accidentale diffusione di informazioni.

In tale direzione, il Codice dell'Amministrazione Digitale (D.Lgs. 82/2005) prescrive all'art. 40 l'obbligo di creazione e gestione dei documenti originali della Pubblica Amministrazione in modalità informatica. Si ricordano a titolo esemplificativo alcune misure utili a proteggere la riservatezza e la disponibilità delle informazioni in formato cartaceo:

- fare ricorso alla stampa solo in caso di reale necessità e comunque il meno possibile;
- in caso di stampa ritirare immediatamente i documenti stampati;
- non lasciare mai incustoditi sul proprio tavolo documenti riservati, anche in caso di assenza breve. In generale riporli in contenitori sottochiave o distruggerli in modo sicuro quando non più utili;
- la distruzione dei documenti in modo sicuro avviene con i "raccoglitori di carta" o strappandoli in piccoli pezzi. Evitare in ogni caso di gettare i documenti interi nel cestino dei rifiuti o del riciclo;
- i documenti devono essere controllati e custoditi dagli utilizzatori fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate negli appositi archivi;

- al termine della giornata lavorativa la propria postazione di lavoro deve essere sgombra da tutti i documenti di tipo riservato e da quelli ad uso interno.

❖ Relativamente alle attività di manutenzione remota su personal computer connessi alla rete scolastica (Didattica/Segreteria), il personale potrà utilizzare specifici software solo su espressa autorizzazione del Dirigente Scolastico.
E' assolutamente vietato utilizzare software che consentono l'accesso diretto ai devices senza una richiesta di autenticazione/codice , i software dovranno essere chiusi al termine delle operazioni di assistenza tecnica, non dovrà in nessun modo essere possibile il collegamento dall'esterno in modalità automatica non vigilata.

CONTROLLI INDIRETTI

1. Controlli

L'Istituto 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 - mirati e non massivi - che consentano di verificare l'effettiva conformità dell'uso degli strumenti informatici alle presenti prescrizioni.

Le verifiche di eventuali situazioni anomale avverranno attraverso le seguenti fasi:

- analisi aggregata del traffico di rete riferito all'intero Istituto o a sue aree (Didattica,Amministrazione e rilevazione della tipologia di utilizzo (e-mail, file, accesso a risorse estranee alle mansioni);
- emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti al settore in cui è stata rilevata l'anomalia;
- in caso di successivo permanere di una situazione non conforme, è possibile effettuare controlli circoscritti su singole postazioni di lavoro.

Con la stessa gradualità vengono effettuati controlli sull'occupazione dello spazio di memorizzazione sui server dell'Istituzione Scolastica attraverso le seguenti fasi:

- analisi aggregata dei dati memorizzati sui servere rilevazione della tipologia di utilizzo (file audio, file video, immagini, software non autorizzato) e relativa pertinenza con l'attività lavorativa;
- emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti , con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti il settore in cui è stata rilevata l'anomalia;
- in caso di successivo permanere di una situazione non conforme, è possibile procedere con un analisi puntuale ed una eventuale eliminazione del materiale non conforme anche sulle singole postazioni di lavoro.

Pertanto, i controlli - proporzionati e non eccedenti anche rispetto allo scopo di verifica dell'adempimento contrattuale - non potranno mai svolgersi direttamente e in modo puntuale, ma saranno preliminarmente compiuti su dati aggregati, riferiti all'intera Istituzione Scolastica o a suoi Uffici.
A seguito di detto controllo anonimo, potrà essere emesso un avviso generalizzato di rilevazione di eventuali anomalie nell'utilizzo dei presidi tecnologici e con l'invito ad attenersi scrupolosamente a

compiti assegnati e alle istruzioni impartite. Se a detta comunicazione non dovessero seguire ulteriori anomalie, L'Istituto 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.

IL DIRIGENTE SCOLASTICO
Dott. re Domenico Balbi
Documento informatico firmato digitalmente
ai sensi del d.lgs. 82/2005 s.m.i. e norme collegate,
il quale sostituisce il documento cartaceo e la firma autografa