"Tra Memoria e Progetto"

LICEO SCIENTIFICO STATALE "NICOLO' PALMERI"
Distretto 8/46 - Piazza Giovanni Sansone, 12 - 90018 Termini Imerese (PA)
**Tel. 091/8144145 - Cod. Mecc. PAPS24000G - C.F. 96030480824**
*e-mail* paps24000g@istruzione.it - paps24000g@pec.istruzione.it - www.liceopalmeri.edu.it

Circ. n. 115

LICEO SCIENTIFICO - "NICOLO' PALMERI"-TERMINI IMERESE
**Prot. 0012200 del 15/11/2022**
III-3 (Uscita)

Termini Imerese, 15/11/2022

A tutto il personale Scolastico

Sito web

# REGOLAMENTO DI UTILIZZO DEGLI STRUMENTI INFORMATICI E DELLA CONNESSIONE AD INTERNET

rivolto a tutti i soggetti a vario titolo coinvolti nell'uso di strumenti e servizi (Docenti, personale amministrativo e collaboratore scolastico, studenti e famiglie, collaboratori esterni fornitori o fruitori di servizi)

## Premesse di buon comportamento

Tutti gli utenti che utilizzano internet devono rispettare:

- La legislazione vigente applicata alla comunicazione su internet
- La netiquette (etica e norme di buon uso dei servizi di rete)

## I vantaggi di internet a scuola

Il curricolo scolastico prevede che **gli studenti** imparino a reperire materiale, recuperare documenti e scambiare informazioni attraverso l'uso delle TIC. Internet offre sia agli studenti sia al **personale docente** una vasta scelta di risorse e opportunità di scambi culturali con persone di altri paesi. Inoltre, su internet si possono recuperare risorse su tempo libero, attività scolastiche e sociali, proposte collaborativo–lavorative.
La scuola propone, sia agli studenti sia al personale docente, di utilizzare internet al fine di promuovere l'eccellenza in ambito didattico, attraverso la condivisione delle risorse, l'innovazione e la comunicazione.
Per gli studenti ed il personale docente l'accesso ad internet è un privilegio ed un diritto. L'accesso ad internet permette al personale docente di svolgere in modo agevole ed efficace diverse funzioni rilevanti da un punto di vista

professionale, in primo luogo l'autoaggiornamento e la partecipazione ad iniziative di e-learning avviate dal Ministero. La possibilità di accedere da scuola alle risorse documentarie tramite internet diviene un fattore imprescindibile per lo svolgimento della professione e per un uso corretto ed efficace delle nuove tecnologie per la didattica.
L'accesso ad internet diventa per gli allievi uno strumento di acquisizione del sapere che si affianca agli strumenti tradizionali e lo rende implicitamente oggetto di particolare attenzione per la formazione dei giovani. L'approccio all'uso delle TIC si presenta quindi come ambito formativo non esclusivamente disciplinare ma trasversale rispetto all'azione educativa dell'istituto.
Esiste però la possibilità che gli studenti trovino materiale inadeguato ed illegale su internet; a tal proposito l'istituto deve prendere opportune precauzioni, limitando l'accesso a internet. Gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività on line, di stabilire obiettivi chiari nell'uso di internet e di insegnarne un uso accettabile e responsabile. L'obiettivo principale resta quello di arricchire ed ampliare le attività didattiche, secondo quanto prevede il curricolo scolastico, l'età e la maturità degli studenti.
Per il **personale ATA**, oltre alle attività legate alle proprie mansioni (trasmissioni telematiche al ministero, monitoraggio progetti, utilizzo della piattaforma di segreteria, etc), l'utilizzo di internet è consentito e promosso per tutte quelle attivitàlegate all'aggiornamento e formazione del proprio profilo professionale.

**Accertamento dei rischi e valutazione dei contenuti di internet**

La scuola si fa carico di tutte le precauzioni necessarie per garantire il divieto di accesso a materiale inappropriato, anche se non è possibile evitare che nessuno si trovi di fronte a materiale inadatto navigando su un computer della scuola.
La scuola non può farsi carico della responsabilità per il materiale trovato su internet o per eventuali conseguenze causate dalla navigazione. Gli studenti imparano ad utilizzare i metodi di ricerca su internet, che includono i cataloghi per soggetto e l'uso dei motori di ricerca. Ricevere e inviare informazioni o messaggi e-mail prevede una buona abilità di gestione delle informazioni e di comunicazione.
Le abilità di gestione delle informazioni includono:

- garanzia di validità, la diffusione e l'origine delle informazioni a cui si accede o che si ricevono;
- utilizzazione di fonti alternative di informazione per proposte comparate;
- ricerca del nome dell'autore, dell'ultimo aggiornamento del materiale e dei possibili altri link al sito;
- rispetto dei diritti d'autore e dei diritti di proprietà intellettuale.

Gli studenti devono essere pienamente coscienti dei rischi a cui si espongono quando sono in rete. Devono essere educati a riconoscere e ad evitare gli aspetti negativi di internet come la pornografia, la violenza, il razzismo e lo sfruttamento dei minori. Agli studenti non deve essere sottoposto materiale di questo tipo e se ne venissero casualmente a contatto dovrebbero sempre riferire l'indirizzo internet (URL) ai responsabili.
Inoltre, l'utilizzo di internet comporta una serie di rischi che possono avere

ripercussioni sulla gestione degli archivi sia di dati comuni sia sensibili:

- rischio interno relativo all'utilizzo della rete da parte di personale non autorizzato ad accedere ai dati;
- rischio esterno dovuto ad intrusioni nel sistema da parte di hacker/cracker;
- rischio interno dovuto ad intrusioni da parte di studenti;
- rischio interno/esterno di scaricamento di virus, Trojan e worm tramite posta elettronica e/o operazioni di download.

**Le strategie della scuola per garantire la sicurezza sull'uso delle TIC**

E' vietato inserire file sul server tranne che in apposite cartelle condivise; è vietato scaricare da internet software non autorizzati.
E' vietato il download di files: è considerato download di file lo scaricamento di materiale digitale da internet o supporti in genere (compresi mini disk, memorie sd, pen drive etc.).
Per utilizzare Pen Drive, CD ROM o altri supporti di memorizzazione personali è necessario chiedere un permesso e sottoporli a controllo antivirus;
In generale, il software utilizzabile è solo quello autorizzato dalla scuola.
Il sistema informatico della scuola è provvisto di software antivirus aggiornato. Ogni utenteche importi dati a scuola tramite supporti esterni è tenuto a verificare l'assenza di virus nel proprio supporto.
La scuola pone in atto le misure preventive in suo possesso, ma ogni utente è informato che, considerata la vastità della problematica, esiste il pericolo reale di infettare il proprio supporto sul sistema della scuola, di conseguenza la scuola declina ogni responsabilità da ogni incidente che possa verificarsi da un eventuale infezione da virus.

Il personale che opera sulle TIC controllerà l'efficacia del sistema di filtraggio. A tal proposito, la strategia della scuola dipende dalle indicazioni previste dal curricolo e dall'età degli studenti in una classe.

**Servizi di posta elettronica**

Il personale durante le attività didattiche non possono utilizzare il servizio e-mail personale se questo interferisce con altre attività di apprendimento. In altri momenti scolastici possono accedere al servizio e-mail personale previa richiesta ai responsabili delle TIC.
Per tutti gli utilizzatori di internet è consentita la consultazione della propria e-mail personale se su dominio istituzionale, istruzione, etc. Non è garantita la consultazione della propria e-mail su dominio privato in quanto potrebbero essere presenti materiali e/o servizi non conformi al presente regolamento.
E' vietato utilizzare catene telematiche di messaggi senza il permesso del mittente;
Il personale che legge i propri messaggi sul server dei servizi di posta non deve lasciarne traccia sui computer dell'istituto; non è consentito configurare un client di posta locale per la lettura di e-mail né al personale docente né agli allievi; solo

in casi particolari e in presenza di una ben precisa programmazione di disciplina, i responsabili delle TIC potranno configurareun client di posta locale per la lettura di e-mail al fine di favorire scambi culturali; il personale non deve rivelare dettagli o informazioni personali loro o di altre persone di loro conoscenza come indirizzi, numeri di telefono od organizzare incontri fuori dalla scuola.

**Gestione del sito della Scuola**

La redazione editoriale della scuola gestisce le pagine del sito ed è sua responsabilità garantire che il contenuto sul sito sia accurato ed appropriato. Il sito assolverà alle linee guida sulle pubblicazioni della scuola. La scuola detiene i diritti d'autore dei documenti che si trovano sul sito, oppure richiede il permesso all'autore proprietario. Le informazioni pubblicate sul sito della scuola relative alle persone da contattare devono includere solo l'indirizzo della scuola, l'indirizzo di posta elettronica e il numero di telefono della scuola ma non informazioni relative agli indirizzi del personale della scuola o altre informazioni del genere.

**Mailing list con moderatore, gruppi di discussione, chat rooms**

L'istituto può utilizzare una lista di indirizzi di utenti selezionati per distribuire del materiale. L'insegnante è il moderatore degli altri mezzi di collaborazione, di mailinglist, di gruppi di discussione e di chat rooms se questi sono utilizzati a scuola. Agli studenti non è consentito l'accesso alle chat rooms, salvo in casi particolari e in presenza di una ben precisa programmazione di disciplina sotto la responsabilità del docente; sono permesse solo chat a scopi didattici; la supervisione del docente è comunque necessaria per garantire la sicurezza; solo i gruppi di discussione che hanno obiettivi e contenuti didattici sono disponibili agli studenti.

**Attacchi esterni**

Sono considerati attacchi esterni tutte quelle attività legate ad individuare vulnerabilità dei sistemi interni o esterni alla scuola e ad utilizzarle per prendere il controllo totale o parziale, per arrecare danni, o solamente per avere accesso a dati non resi volontariamente pubblici. La scuola vieta espressamente tale tipologia di attività.

**Servizi on line agli utenti esterni**

All'interno del proprio sito web, la scuola offre servizi alle famiglie e agli utenti esterni:

- orari delle classi, dei docenti, degli uffici e delle strutture;
- comunicazioni alle famiglie;
- modulistica;
- tramite l'accesso al sito del registro elettronico, valutazioni degli allievi (accesso riservato all'utenza tramite nome utente e password personali).

Tali servizi sono erogati in conformità con quanto espresso della Legge 196/2003 in materia del trattamento dei dati.

**Informazioni per i genitori / tutori**

I genitori / tutori vengono informati delle regole dell'uso internet dell'istituto sul sito web della scuola; è auspicabile che le regole sull'uso accettabile e responsabile di internet all'interno dell'istituto siano condivise e conseguite dalle famiglie anche nell'ambiente domestico.
Eventuali commenti o suggerimenti connessi possono essere inviati all'attenzione del Dirigente Scolastico.

**Informazioni per il personale scolastico**

Il personale scolastico viene informato della regole dell'acceso ad internet dell'istituto sul sito web della scuola; è inoltre consapevole che l'uso di internet verrà monitorato e segnalato e che tutto il personale scolastico sarà coinvolto nello sviluppo del regolamento di utilizzo della rete della scuola e nell'applicazione delle istruzioni sull'uso sicuro e responsabile di internet.
In caso di dubbi legati alla legittimità di una certa istanza utilizzata in internet, il personale dovrà contattare il Dirigente scolastico per evitare malintesi.

## *REGOLAMENTO UTILIZZO SISTEMI INFORMATIVI*

### Art. 1 Oggetto e ambito di applicazione

Il presente regolamento e le sue premesse che ne sono parte integrante, disciplinano le modalità di accesso, di uso delle risorse informatiche dell'Istituto dell'Istituzione scolastica (rete, apparecchiature e risorse infrastrutturali, patrimonio informativo e software).
Le risorse infrastrutturali sono le componenti hardware/software e gli apparati elettronici collegati alla rete informatica della scuola. Il patrimonio informativo è l'insieme delle banche dati in formato digitale e in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati. Le risorse software sono i sistemi operativi e i programmi acquisiti legalmente dall'Istituto).

Il presente regolamento si applica a tutti gli utenti interni che sono autorizzati ad accedere alla rete della scuola: impiegati amministrativi, docenti, collaboratori scolastici. Si applica anche a taluni utenti esterni, quali i collaboratori esterni, ditte fornitrici di software che effettuano attività di manutenzione limitatamente alle applicazioni di loro competenza, ditte fornitrici di hardware o delegate alla sua manutenzione (è consentita la visualizzazione di files solo per quanto strettamente indispensabile), eventuali enti esterni autorizzati da apposite convenzioni

all'accesso a specifiche banche dati con le modalità stabilite dalle stesse.

## Art. 2 Principi generali – Diritti e Responsabilità

Ogni utente è responsabile civilmente e penalmente del corretto uso delle risorse informatiche, dei servizi/programmi ai quali ha accesso e dei propri dati. Tutti i soggetti interagenti, a qualunque titolo, col sistema informatico dell'Istituto sono anche responsabili di eventuali danni erariali conseguenti.
Per motivi di sicurezza e protezione dei dati, ogni attività compiuta nella rete informatica è sottoposta a registrazione in files-registro; la registrazione riguarda orario di inizio e fine dell'accesso al sistema e all'account che ha operato. Detti files possono essere soggetti a trattamento solo per fini istituzionali, per attività di monitoraggio e controllo; possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazione della normativa vigente. La riservatezza delle informazioni in essi contenute è soggetta a quanto dettato dal DLgs. n. 196/2003 e normativa collegata.
L'Istituto, per fini legati alla sicurezza dell'intero sistema informativo, dispone di strumenti per il monitoraggio e il controllo della navigazione in internet.

## Art. 3 Utilizzo dei personal computer

Il personal computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività professionale può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Pertanto:

**a)** L'uso dell'elaboratore con profilo di accesso specifico (utenti dell'area Amministrativa e di Sistema, Sistema integrato del registro elettronico, piattaforma di e-Learning, account individuali riservati) deve essere protetto da password e non divulgata. Gli account destinati al trattamento di dati amministrativi e sensibili sono custoditi a cura del Titolare del trattamento dati.

**b)** Il Dirigente Scolastico e/o preposti all'amministrazione del sistema, nell'espletamento delle funzioni legate alla sicurezza e alla manutenzione informatica etc., avranno la facoltà di accedere in qualunque momento anche da remoto a tutte le postazioni e a tuttigli account.

**c)** Il personal computer deve essere spento **al termine dell'orario delle lezioni o di servizio**, comunque prima di lasciare gli uffici, i laboratori di informatica, le aule. 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 termine di qualunque sessione riservata di lavoro o di assenza temporanea è obbligatorio uscire dall'account o bloccare il computer.

**d)** è vietato installare autonomamente programmi informatici **sui server** e sui Pc

salvo autorizzazione esplicita del Dirigente Scolastico e/o del Direttore S.G.A. L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre la struttura a gravi responsabilità civili ed 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;

**e)** è vietato modificare le caratteristiche impostate sul proprio Pc, salvo con autorizzazione esplicita degli amministratori di sistema o del Dirigente Scolastico;

**f)** è vietato inserire password locali alle risorse informatiche assegnate (come ad esempio password che non rendano accessibile il computer agli amministratori di rete), se non espressamente autorizzati e dovutamente comunicate agli amministratori di sistema;

**g)** É vietata l'installazione sul proprio Pc di dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, dischi esterni, i- pod, telefoni, ecc.), se non con l'autorizzazione esplicita del Dirigente Scolastico e/o del Direttore S.G.A. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente gli amministratori di sistema e/o il Dirigente Scolastico nel caso in cui vengano rilevati virus o eventuali malfunzionamenti.

**h)** è vietato spostare Pc senza autorizzazione del Dirigente Scolastico e/o del Direttore S.G.A.

**i)** È vietato collegare in rete personal computer portatili non di proprietà della scuola, salvo diversa ed esplicita autorizzazione avuta dall'Amministratore di Sistema e/o dal Dirigente Scolastico.

## Art. 4 Utilizzo della rete informatica

Le unità di rete sono aree di condivisione di informazioni strettamente professionali sulle quali vengono svolte regolari attività di controllo, amministrazione e backup 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 in queste unità.

In presenza di reti locali con dominio, i files relativi alla produttività individuale possono essere salvati sul server e i limiti di accesso sono regolarizzati da apposite procedure di sicurezza che suddividono gli accessi tra gruppi e utenti aventi profili di autorizzazione diversi.

Gli amministratori di sistema possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza o in violazione del presente regolamento sia sui Pc degli incaricati sia sulle unità di rete.
Costituisce buona regola la periodica **pulizia degli archivi**, con cancellazione dei files obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. è infatti assolutamente da evitare un'archiviazione ridondante.
E' importante togliere tutte le condivisioni dei dischi o di altri supporti configurate nel Pc se non strettamente necessarie (e per breve tempo) allo scambio dei file con altri colleghi. Esse sono infatti un ottimo "aiuto" per i software che cercano di minare la sicurezza dell'intero sistema.
E' compito degli amministratori di sistema provvedere alla creazione e alla manutenzione di aree condivise sul server per lo scambio dei dati tra i vari utenti.
Nell'utilizzo della rete informatica È fatto divieto di:

**a)** Utilizzare la Rete in modo difforme da quanto previsto dal presente regolamento;

**b)** Agire deliberatamente con attività che influenzino negativamente la regolare operatività della Rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;

**c)** Effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc);

**d)** Installare componenti hardware non compatibili con l'attività istituzionale;

**e)** Rimuovere, danneggiare o asportare componenti hardware;

**f)** Utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare file e software di altri utenti;

**g)** Utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di intercettazione di tastiera (keygrabber o keylogger), software di decodifica password (cracker) e più in generale software rivolti alla violazione della sicurezza del sistema e della privacy.

## Art. 5 Utilizzo di internet

I Pc abilitati alla navigazione in Internet costituiscono uno strumento necessario e prezioso per lo svolgimento dell'attività professionale.
Nell'uso di internet e della posta elettronica non sono consentite le seguenti attività:

**a)** L'uso di internet per motivi personali (ad esempio facebook).

**b)** L'accesso a siti inappropriati (esempio siti pornografici, di intrattenimento, ecc.);

**c)** Lo scaricamento (download) di software e di file non necessari all'attività istituzionale, sia perchè potrebbero celare minacce al buon funzionamento del sistema, sia perchè software privi di licenza comportano gravissime sanzioni economiche e penali per il Datore di lavoro ed eventualmente anche per il dipendente;

**d)** Utilizzare programmi per la condivisione e lo scambio di file (Napster, Emule, Winmx, e-Donkey, ecc.);

**e)** Accedere a flussi in streaming audio/video da Internet per scopi non istituzionali;

**f)** Un uso che possa in qualche modo recare qualsiasi danno all'Istituto o a terzi.

Il dipendente non deve eseguire download di files eseguibili o documenti da siti Web, HTTP o FTP non conosciuti. Si ricorda che la frequentazione di siti non conosciuti o lo scaricamento di files da fonti non garantite possono introdurre virus o altro malware, che possono creare inconvenienti gravissimi, con perdita di dati, blocco operativo e danni economici importanti. L'imprudente autore può essere chiamato a risponderne in via disciplinare e per il danno recato.

## Art. 6 Utilizzo della posta elettronica

La casella di posta assegnata dall'Istituto, è uno strumento di lavoro e le persone assegnatarie delle caselle di posta elettronica sono responsabili del loro corretto utilizzo.
É fatto divieto di utilizzare le caselle di posta elettronica della struttura per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione, che esulino dagli scopi della scuola.
É buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali con l'istituto ricevuta da personale non autorizzato, deve essere visionata ed inoltrata al Direttore SGA, o in ogni caso è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.
La documentazione elettronica che viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto, non può essere comunicata all'esterno senza preventiva autorizzazione del Responsabile del trattamento.
Per la trasmissione di files all'interno della struttura è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati (ad esempio per dimensioni superiori a 2 MB È preferibile utilizzare le cartelle di rete condivise).

E’ obbligatorio controllare i file attachments (allegati) di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web, HTTP o FTP non conosciuti) e accertarsi dell’identità del mittente.
In particolare nell’uso della posta elettronica non sono consentite le seguenti attività:

**a)** La trasmissione a mezzo di posta elettronica di dati sensibili, confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali e inerenti le ragioni di servizio;
**b)** L’apertura di allegati ai messaggi di posta elettronica senza il previo accertamento dell’identità del mittente;
**c)** Inviare tramite posta elettronica informazioni quali user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici.

## Art. 7 Utilizzo delle password

Le password sono previste ed attribuite dai referenti di sistema, ovvero dal Titolare del trattamento dei dati.
E’ necessario procedere alla modifica della password almeno ogni tre mesi (come previsto dal disciplinare tecnico allegato al Codice della privacy, GDPR n.679/2016) con contestuale comunicazione all’Incaricato della custodia delle Password.
La comunicazione di variazione delle password dovrà essere consegnata al “Custode delle password” ( D.S.G.A ), in busta chiusa, con data, nome e firma dell’incaricato apposte sul lembo di chiusura.
Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all’incaricato (disciplinare tecnico Privacy). La password dev’essere modificata ogni 3 mesi se il computer consente l’accesso a dati sensibili, altrimenti ogni 6 mesi. La password non deve essere scritta su supporti cartacei. Nel caso si sospetti che la password abbia perso la segretezza, deve essere immediatamente sostituita, dandone comunicazione scritta all’Incaricato della custodia delle Password.
Qualora l’utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia, per iscritto, al Titolare.

## Art. 8 Utilizzo dei supporti magnetici

Tutti i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD e DVD) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato (disciplinare tecnico Privacy). Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
I supporti magnetici contenenti dati sensibili (disciplinare tecnico Privacy) devono

essere custoditi in archivi chiusi a chiave.
Tutti i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili e DVD) obsoleti devono essere consegnati agli Amministratori di Sistema per l'opportuna distruzione.
Ogni qualvolta si procederà alla dismissione di un Personal Computer gli Amministratori di Sistema provvederanno alla distruzione o all'archiviazione protetta delle unità di memoria interne alla macchina stessa (hard-disk, memorie allo stato solido).

**Art. 9 Utilizzo di pc portatili**

L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
I PC portatili utilizzati all'esterno (convegni, lavoro domestico autorizzato, ecc…), in caso di allontanamento devono essere custoditi in un luogo protetto.

**Art. 10 Utilizzo delle stampanti e dei materiali di consumo**

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, floppy disk, supporti digitali come CD e DVD) è riservato esclusivamente ai compiti di natura strettamente istituzionale.
Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.
É cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. É buona regola evitare di stampare documenti o file non-adatti (molto lunghi o non- s u p p o r t a t i, come ad esempio files di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

IL DIRIGENTE SCOLASTICO
Prof.ssa Marilena Anello
(Documento firmato digitalmente)