ISTITUTO STATALE D'ISTRUZIONE SECONDARIA SUPERIORE - "RINALDO D'AQUINO"-MONTELLA
Prot. 0002390 del 01/04/2023
I-1 (Uscita)

ISTITUTO D'ISTRUZIONE SUPERIORE
"RINALDO D'AQUINO"

e-mail: *avis02100b@istruzione.it* ***P.E.C.*** *avis02100b@pec.istruzione.it* **C.F. 91010430642**

hirpina audacia

Liceo Scientifico – Liceo delle scienze umane
via Scandone – 83048 – Montella
Segreteria: 0827-1949166 fax: 0827-1949162
Uff. Dirigente Scolastico: 0827 1949161
Liceo Classico
via Fontanelle, 1 - 83051 – Nusco 0827 64972
I.P.I.A. e I.T.I.S.
ind. Elettronica , chimico-biologico, Informatica e Telecomunicazioni
Via Verteglie – 83048 - Montella 0827 1949183 - fax 0827 1949182
Istituto Tecnico Industriale ind. Meccanica, meccatronica ed energia
Via Tuoro - Bagnoli Irpino- tel 0827 62268

ISTRUZIONI OPERATIVE UTILIZZO SISTEMI INFORMATICI

INDICE

PREMESSA
UTILIZZO DEL PERSONAL COMPUTER
UTILIZZO DELLA RETE
GESTIONE DELLE PASSWORD
UTILIZZO DEI SUPPORTI DI MEMORIZZAZIONE
UTILIZZO DI PC PORTATILI
UTILIZZO DEI LABORATORI E DELLE APPARECCHIATURE INFORMATICHE AD USO DIDATTICO
ACCESSO AD INTERNET E USO DELLA POSTAZIONE DI LAVORO
USO DI INTERNET
UTILIZZO DELLE RETE INTERNET PER USO DIDATTICO
USO DELLA POSTA ELETTRONICI
OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY.

PREMESSA

L'utilizzo delle risorse informatiche e telematiche del nostro Istituto deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro. L'Istituto ha adottato una procedura interna diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato al personale è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata.

Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del *Responsabile dei sistemi informatici*, in quanto sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.
Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal *Responsabile dei sistemi informatici.* L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Istituto a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita del *Responsabile dei sistemi informatici*.
Il Personal Computer deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio.
Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro, se non con l'autorizzazione espressa del *Responsabile dei sistemi informatici.*
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il *Responsabile dei sistemi informatici* nel caso in cui vengano rilevati virus.

UTILIZZO DELLA RETE

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. 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 backup.
Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
Il *Responsabile dei sistemi informatici* può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
Costituisce buona regola la periodica pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

GESTIONE DELLE PASSWORD

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal *Responsabile dei sistemi informatici.*

È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati particolari (ex dati sensibili) e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al *Responsabile dei sistemi informatici.*

Le password possono essere formate da lettere (maiuscole o minuscole), simboli 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.

La password deve essere immediatamente sostituita, dandone comunicazione al *Responsabile dei sistemi informatici*, nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al *Responsabile dei sistemi informatici*.

UTILIZZO DEI SUPPORTI DI MEMORIZZAZIONE

Tutti i supporti di memorizzazione riutilizzabili (pennette usb, cd, dvd, ecc.) contenenti dati particolari (ex dati sensibili) e giudiziari devono essere trattati con particolare cautela per esempio crittografando i dati, onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti di memorizzazione contenenti dati particolari (ex dati sensibili) e giudiziari devono essere custoditi in armadi o cassetti sicuri chiusi a chiave.

UTILIZZO DI PC PORTATILI

L'utente è responsabile del PC portatile assegnatogli dal *Responsabile dei sistemi informatici* 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, visite in altri Istituti, ecc…) devono essere custoditi in un luogo protetto.

UTILIZZO DEI LABORATORI E DELLE APPARECCHIATURE INFORMATICHE AD USO DIDATTICO

L'uso dei laboratori e/o delle apparecchiature informatiche è finalizzato esclusivamente all'attività didattica.

Sono da considerarsi apparecchiature del laboratorio informatico: le macchine fotografiche, le videocamere, i PC, i tablet, le stampanti, gli scanner, le unità di memorizzazione esterne.

Al laboratorio e/o alle apparecchiature possono accedere, in ordine di priorità:

- Le classi che, accompagnate dai docenti, svolgano attività di elaborazione dati, esercitazioni o visione di programmi didattici multimediali o ricerche in Internet;
- I docenti per attività connesse con l'aggiornamento e l'insegnamento.

Gli alunni possono accedere alle macchine o ai laboratori solo se accompagnati da un insegnante, che ne ha la responsabilità. Il docente non può lasciare da soli gli alunni in laboratorio o durante l'uso delle apparecchiature.

E' fatto assoluto divieto di:

- Installare sui PC programmi personali.
- Installare e utilizzare programmi privi della relativa licenza d'uso.
- Portare fuori dalla scuola i programmi originali di cui la scuola è dotata.

Non è consentito modificare le impostazioni dei computer (aspetto del desktop, salvaschermi, suoni, caratteri, ecc) se non per motivi didattici. Le impostazioni di default devono essere ripristinate al termine della lezione.

Ogni docente deve salvare il proprio lavoro didattico e/o quello degli alunni su supporti esterni o su cartelle ordinate, secondo le modalità concordate con il *Responsabile dei sistemi informatici*.

ACCESSO AD INTERNET E USO DELLA POSTAZIONE DI LAVORO

La configurazione dei servizi di accesso a internet e alla posta elettronica viene eseguita esclusivamente dai tecnici incaricati, e può essere affidato a Ditta esterna all'Amministrazione o al personale interno delegato.

Le postazioni di lavoro del personale amministrativo sono preventivamente individuate e assegnate a ciascun dipendente.

Per accedere ai servizi informatici della scuola dalla postazione di lavoro e per garantirne la sua protezione, il personale amministrativo dovrà utilizzare una password.

Tutti i dipendenti si impegnano a:

1) Non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a personale non autorizzato, in particolare per quanto riguarda l'accesso ai servizi di posta elettronica;

2) Mantenere la corretta configurazione del proprio computer non alterando le componenti hardware e software predisposte allo scopo né installando software non autorizzati;

3) Non installare o non utilizzare programmi di sistema, applicativi o gestionali privi di regolare contratto di licenza d'uso;

4) Sottoporre a controllo preventivo tutti i files di provenienza incerta o esterna, attinenti all'attività lavorativa;

5) Non scaricare files contenuti in supporti di memorizzazione che non abbiano attinenza con la propria prestazione lavorativa.

Per non limitare le attività tipicamente scolastiche, non è definito a priori un elenco di siti autorizzati; è tuttavia obbligatorio l'utilizzo di adeguati strumenti di filtraggio, con i quali può essere bloccata la navigazione su categorie di siti i cui contenuti sono stati classificati come certamente estranei agli interessi ed alle attività lavorative.

USO DI INTERNET

Tutti i dipendenti possono utilizzare Internet.

Il dipendente-utente è direttamente e totalmente responsabile dell'uso che egli fa del servizio di accesso ad Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.

L'uso di Internet nelle numerose funzionalità è consentito esclusivamente per scopi attinenti alle proprie mansioni.

Al dipendente non è consentito:

- Caricare/scaricare (upload/download) da Internet files musicali, video o software che non siano attinenti alla propria mansione, come anche l'utilizzo di connessione ad Internet per motivi strettamente personali, in quanto ciò si configura come danno patrimoniale cagionato all'Amministrazione consistente nel mancato svolgimento della prestazione lavorativa durante il periodo di connessione;
- L'utilizzo delle risorse dei sistemi informatici dell'Istituto per la memorizzazione di materiale di uso privato, personale o non attinente alla attività lavorativa;
- Effettuare transazioni finanziarie, operazioni di remote banking, acquisti on-line e simili, se non attinenti l'attività lavorativa o direttamente autorizzati dal Responsabile;
- Utilizzare sistemi Peer to Peer, di file sharing, podcasting, web casting, eMule, utorrent e similari, così come connettersi a siti che trasmettono programmi in streaming (come radio e TV via web) senza essere preventivamente autorizzati dal Responsabile;
- Usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti in rete;
- Scaricare software gratuiti senza aver verificato il rispetto delle condizioni di licenza e la sicurezza del download
- Partecipare a forum e/o utilizzare chat se non per motivi strettamente attinenti l'attività lavorativa.

UTILIZZO DELLE RETE INTERNET PER USO DIDATTICO

Gli insegnanti sono tenuti ad una stretta sorveglianza degli alunni durante la navigazione in internet per evitare che – a causa di improvviso ed imprevedibile mal funzionamento dei filtri – possano accedere a siti non adeguati.

Nel caso si verifichi una tale evenienza, gli insegnanti sono tenuti ad interrompere immediatamente la navigazione e a segnalare il fatto ai docenti responsabili.

Per evitare che si verifichi l'accesso a siti impropri, gli insegnanti sono tenuti a:

- Visionare anticipatamente i siti su cui intendono lavorare con gli alunni;
- Far eseguire ricerche esclusivamente attraverso i motori di ricerca interni a siti di navigazione sicura per bambini/ragazzi

- .

USO DELLA POSTA ELETTRONICA

La casella di posta istituzionale è uno **strumento di lavoro**. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse

Tutti gli utenti dovranno valutare attentamente, prima di aprirli, i messaggi che provengono sulla propria casella di posta elettronica, in caso di mail di dubbia provenienza, gli allegati non dovranno essere aperti.

Al dipendente non è consentito:

- Utilizzare la posta elettronica istituzionale per motivi non attinenti alle mansioni assegnate;
- Utilizzare l'indirizzo di posta elettronica istituzionale per la partecipazione a dibattiti, forum e mail-list, salvo specifica autorizzazione in tal senso da parte del responsabile;
- Aprire gli allegati di non comprovata origine in assenza di software antivirus aggiornato sulla propria postazione di lavoro;
- Effettuare chiamate a link contenuti all'interno di messaggi a meno di comprovata sicurezza sul contenuto dei siti richiamati;
- Rispondere ad e-mail pervenute da mittenti sconosciuti. Nel dubbio si suggerisce di cancellarle preventivamente;
- Utilizzare il servizio di posta per inoltrare giochi, scherzi, barzellette, appelli e petizioni e altre e-mail che non siano di lavoro;
- Allegare al testo delle comunicazioni materiale insicuro o files di dimensioni eccessive.

Si raccomanda di prestare particolare attenzione ai messaggi di phishing, ossia messaggi di posta contenenti link a siti che mirano ad estorcere le credenziali di accesso ai sistemi informatici.

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure adeguate di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

DIRIGENTE
SCOLASTICO
Dott.ssa Emilia STROLLO
(Firma autografa omessa ai sensi dell'art. 3del D.lgs39/1993)