Regole di comportamento al PC

Sono di seguito riportate le modalità di comportamento e raccomandazioni al fine di evitare la perdita di dati e/o intrusioni all'interno del Sistema Informatico.

✓ Protezione dei dati [Accesso a windows e Password]

1) Assicurarsi che sia sempre attiva la **Password** di accesso al Sistema operativo→ in caso di esito negativo contattare il **Responsabile Sistema informatico;**
2) Assicurarsi che sia attivo il proprio **Screen Saver con password** di ripristino nel caso si lasci il PC acceso (max 10 minuti di inattività);
3) La **password** deve essere costituita da una sequenza di **minimo otto caratteri** alfanumerici e **s** deve essere facilmente individuabile (es. cognome, data di nascita, etc.); Non deve contenere lo user-id e, in generale, riferimenti riconducibili al possessore come parte della password. Buona norma è che una parte dei caratteri che costituiscono la password sia di natura numerica, contenga almeno un carattere speciale ed una lettera maiuscola;
4) La password va cambiata con periodicità **almeno semestrale**; la nuova password **NON** deve essere simile alla password precedente;
5) La password **NON** deve essere comunicata ad altri; qualora si renda necessario va conseguentemente cambiata informando (anche a mezzo mail) il **Dirigente Scolastico e i suoi delegati.**

✓ Divieti e precauzioni

▪ SOFTWARE

6) È fatto divieto di **installare software** di qualsiasi tipo sui personal computer al di fuori di quello strettamente necessario per lo svolgimento **delle attività scolastiche e per le quali l'Istituto ha la relativa licenza d'uso;**
7) In particolare è fatto divieto di **installare** sui personal computer software per **accesso remoto** (teamviewer o simili) fornendo la password a Società (anche se esterne incaricate dall'IC senza preventiva autorizzazione della Direzione;
8) Evitare l'uso di **programmi shareware** e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di "scaricare" dalla rete internet ogni sorta di file, eseguibile e non eseguibile.

   → in caso di necessità avvisare il Responsabile sistema informatico dell'Istituto o in sua assenza il DS / DGSA

▪ MAIL

9) **NON** aprire gli **allegati di posta** se **non si è certi** della loro provenienza (Mittente non conosciuto!); Qualora riportino link a pagine esterne non cliccare in alcun modo su tali link anche se il messaggio indica nell'oggetto "aggiorna/conferma le tue informazioni" o frasi simili → **cancellare tali mail**
10) **Non** fornire mai i propri dati su richieste esterne a mezzo e-mail in particolare dati bancari (**le banche o altri enti non chiedono mai i vs dati a mezzo e-mail**)

▪ MALFUNZIONAMENTI

11) Seguire scrupolosamente le istruzioni fornite dal **sistema antivirus** nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto)
12) Avvisare il **Resp. SI** nel caso in cui si riscontri un **qualche anomalo malfunzionamento** del proprio PC quale ad es. apertura in automatico di **determinati link** a siti mentre si naviga col proprio Browser (Internet Explorer – Chrome - Mozzilla firefox) o finestre del sistema operativo o un **peggioramento improvviso delle prestazioni** (velocità di apertura di software o di navigazione)

▪ CONDIVISIONE CARTELLE, FILE – UTILIZZO DI USB

13) **Non** attivare le **condivisioni** dell'HD (Disco C) in scrittura; qualora si debba condividere una o più cartelle accertarsi di non aver condiviso erroneamente tutto il disco C;
14) **Non** copiare in alcun modo, senza autorizzazione esplicita del Direzione Aziendale, file aziendali su propri supporti USB o Hard-disk.

✓ Attività di controllo

15) Controllare (**scansionare con un antivirus aggiornato**) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
16) Assicurarsi che sia attivo l'**antivirus** e che la "firma dei virus" risulti aggiornata ad un periodo non superiore ai 30 gg;
17) Controllare le **notifiche** del Sistema Operativo (azioni consigliate) ed in caso di dubbi contattare la Direzione;
18) Non utilizzare **social software** quali Facebook, Instagram, Twitter; **attività consentita solo nelle pause lavorative.**

Camerino li 09/09/2024

Il Dirigente Scolastico IL DIRIGENTE SCOLASTICO
Prof. Francesco Rosati

Via medici 12 Camerino 62032 (MC) – tel. +39 0737 434965 – mcic809009@istruzione.it
PEC: mcic809009@pec.istruzione.it – codice meccanografico: MCIC809009- codice fiscale: 9001170439