



Ministero dell'Istruzione, dell'Università e della Ricerca
UFFICIO SCOLASTICO REGIONALE PER LA CAMPANIA
ISTITUTO COMPRENSIVO
"Raffaele Iozzino"

Via Roma n. 37 - 80050 Casola di Napoli (Na) Tel: 081 8012889; Fax: 081 3905896; C.M. NAIC8AG00A
E-mail: naic8ag00a@istruzione.it; naic8ag00a@pec.istruzione.it; c.f. 82013140635; www.icraffaeleiozzino.gov.it



Prot. n. 1722/VI-11 del 17/09/2018

Casola di Napoli,

SITO WEB

Registro elettronico

A tutto il personale docente ed Ata

p.c.al DSGA

Istruzioni operative interne circa l'utilizzo a scopo lavorativo di strumenti informatici assegnati al personale

Il presente Regolamento ha l'obiettivo di regolamentare l'utilizzo degli strumenti informatici, ossia definire in modo puntuale le regole e i confini da non superare nell'uso delle dotazioni.

Tenuto conto delle Linee guida sulla disciplina della navigazione in Internet e sulla gestione della posta elettronica nei luoghi di lavoro emanate dal Garante per la Privacy, con propria deliberazione n. 13 del 1 marzo 2007, il personale deve attenersi alle seguenti istruzioni e raccomandazioni nell'utilizzo del personal computer.

- Il personal computer con i relativi programmi, il telefono, i fax e ogni altro bene della scuola costituiscono strumenti di lavoro il cui utilizzo ricade sotto la responsabilità della scuola stessa, che li mette a disposizione del proprio personale a condizione che vengano custoditi con cura dal dipendente cui sono assegnati, evitando manomissioni, danneggiamenti o utilizzi, anche da parte di altre persone, per scopi non consentiti.
- Non è consentito modificare le configurazioni impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come, ad es., masterizzatori, modem, ecc.).
- Sui personal computer o tablet dotati di scheda audio e/o di lettore CD non è consentito l'ascolto di programmi, file audio o musicali, se non a fini prettamente lavorativi.
- Il personal computer o tablet deve essere protetto da password di accensione, che deve essere attivata anche per il disco fisso. Lo screensaver deve essere impostato per tempi brevi (15 minuti) e, quando attivato, disinseribile solo tramite password utente.
- Il personal computer deve essere **spento** prima di lasciare gli uffici e le aule scolastiche e in caso di assenze prolungate 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.
- Non è consentito utilizzare programmi diversi da quelli ufficialmente installati né 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.
- Non è consentito scaricare file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.
- Tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo da parte di personale tecnico qualificato in materia.(Prof. de Lisio, Prof. Verdoliva)
- Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale addetto nel caso in cui siano rilevati virus e seguendo le procedure di protezione antivirus.



Ministero dell'Istruzione, dell'Università e della Ricerca
UFFICIO SCOLASTICO REGIONALE PER LA CAMPANIA
ISTITUTO COMPRENSIVO
"Raffaele Iozzino"



Via Roma n. 37 - 80050 Casola di Napoli (Na) Tel: 081 8012889; Fax: 081 3905896; C.M. NAIC8AG00A
E-mail: naic8ag00a@istruzione.it; naic8ag00a@pec.istruzione.it; c.f. 82013140635; www.icraffaeleiozzino.gov.it

- Tutti i supporti magnetici rimovibili (floppy disk, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni, sono vietati onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
- Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale addetto e seguire le istruzioni da questo impartite.
- In ogni caso, i supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dagli utenti in armadi chiusi.
- È vietato l'utilizzo di supporti rimovibili personali.
- L'utente è responsabile della custodia dei supporti e dei dati della scuola in essi contenuti.
- Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dall'incaricato delle credenziali, previa formale richiesta del Responsabile dell'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.
- Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (User Id), assegnato dal personale addetto, associato ad una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata.
Non è consentita l'attivazione della password di accensione senza preventiva autorizzazione da parte del personale addetto.
- È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi.
- 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 l'incaricato delle credenziali, soggetto preposto alla custodia delle credenziali di autenticazione.
- 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 e ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.
- Le unità di rete 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.**
- La scuola si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione del presente Regolamento/ Codice di condotta.
- Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante

IL DIRIGENTE SCOLASTICO
f.to Prof.ssa Maria Gargiulo