

POLICY PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI NEL LICEO COLONNA DI GALATINA"

Scopo: dettare le procedure per una corretta e adeguata gestione del patrimonio informativo all'interno dell'Istituto.

NORME DI RIFERIMENTO

- A) la Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento"; in particolare l'art. 4, comma 1, della Legge 300/1970, secondo cui la regolamentazione dell'uso degli strumenti informatici non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali;
- B) il Regolamento Europeo 679/16 "General Data Protection Regulation" (d'ora in avanti Reg. 679/16 o GDPR); in particolare viene garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Reg. 2016/679;
- C) le "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- D) l'articolo 23 del D.lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa».

PREMESSE

- A) **Tutti gli strumenti utilizzati dal lavoratore**, quali PC, notebook, e-mail ed altri strumenti (di seguito più semplicemente "strumenti informatici"), **sono messi a disposizione dall'Ente unicamente per svolgere la propria attività lavorativa.**
- B) **Tutti gli strumenti informatici** affidati ai dipendenti, compreso il PC, **sono strumenti di lavoro.** Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
- C) Occorre che il dipendente/incaricato sia ben consapevole che gli Strumenti forniti sono di proprietà dell'Ente e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa.

REGOLAMENTO

1. **Non è consentito installare autonomamente programmi provenienti dall'esterno** salvo previa autorizzazione esplicita dell'amministratore di sistema/Dirigente Scolastico, in quanto sussiste il grave pericolo di portare virus e di creare rischi seri per la sicurezza informatica.
2. **Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati** ufficialmente sui PC. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente,

può esporre la scuola a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software. A tal riguardo si ricorda come la scuola metta a disposizione la piattaforma GWorkspace che offre una suite di programmi molto ampia (Documenti, Presentazioni, Sheet, Jamboard, My Maps, Calendar, Meet, Earth, Keep).

3. **Non è consentito all'utente modificare le caratteristiche impostate sul PC dell'aula o sul Notebook affidato dal Dirigente Scolastico**, salvo previa autorizzazione esplicita dell'amministratore di sistema/Dirigente Scolastico. Il personal computer, inoltre, deve essere spento alla fine dell'ultima ora di lezione e comunque prima di lasciare il plesso scolastico. Il Notebook preso per attività didattica va riconsegnato all'incaricato del laboratorio per riporlo in un luogo sicuro.
4. **L'accesso agli strumenti è protetto da password**; a) per l'accesso devono essere utilizzati Username e password assegnate dall'Amministratore di Sistema per quanto concerne il Registro Elettronico e la piattaforma GWorkspace. A tal proposito si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza. A tal proposito si rammentano le conseguenze di detto comportamento "apparentemente innocuo" e le responsabilità che ne derivano. b) I Pc/notebook presenti nelle aule e nei locali della scuola sono protetti da password (senza Username). Anche per tale password valgono le regole di conservazione e riservatezza indicate nel comma precedente.
5. Per quanto riguarda la casella di posta elettronica della scuola, ci si richiama al senso di responsabilità di ciascun dipendente/collaboratore e in particolare porre attenzione alle seguenti considerazioni: a) Occorre precisare che **la casella di posta, assegnata dalla scuola all'utente, è uno strumento di lavoro**. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. b) Ad ogni utente viene fornito un account e-mail nominativo quale nome.cognome@dominio della scuola. c) **L'utilizzo dell'e-mail deve essere limitato esclusivamente per scopi lavorativi, ed è assolutamente vietato ogni utilizzo di tipo privato**. L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa; d) E' vietato **utilizzare la caselle di posta elettronica della scuola per l'invio di messaggi personali** o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione, e) È buona norma **evitare messaggi completamente estranei al rapporto di lavoro** o alle relazioni tra colleghi.
6. **In caso di cessazione del rapporto lavorativo, la mail affidata all'incaricato verrà disattivata immediatamente.**
7. **Uso della rete internet:** ricordando che l'utilizzo della rete deve sempre essere indirizzato allo svolgimento di mansioni legate alle funzioni svolte in questa istituzione, occorre fare attenzione al download e all'upload di file e software al fine di tutelare tutta la rete della scuola dall'accesso indiscriminato a siti non sicuri.
8. Qualora il docente decida di adottare la metodologia BYOD, Bring Your Own Device, deve tenere ben presente che "È ... consentito l'utilizzo di tali dispositivi in classe, quali strumenti compensativi di cui alla normativa vigente, nonché, in conformità al Regolamento d'istituto, con il consenso del docente, per finalità inclusive, didattiche e formative, anche nel quadro del Piano Nazionale Scuola Digitale e degli obiettivi della c.d. "cittadinanza digitale" di cui all'art. 5 L. 25 agosto 2019, n. 92." in base alla nota ministeriale 0107190 del 19 dicembre 2022 Per tale fine l'azienda deve

concedere al dipendente di accedere alla rete informatica interna andando a creare una nuova area di rischio che deve essere costantemente monitorata.

9. **Protezione antivirus:** in caso in cui l'utente venga avvisato da segnalazioni di anomalie provenienti dal software antivirus presente sul pc deve immediatamente avvisare il proprio amministratore di sistema/Dirigente Scolastico che analizzerà l'accaduto e prendere gli opportuni provvedimenti.
10. **Dal momento che le chiavette USB possono essere veicolare facilmente virus arrecando danni ai sistemi informatici, si raccomanda di caricare i file della chiavetta sulla cloud d'Istituto (il Drive di GWorkspace).**
11. **Appena si lascia una postazione, ricordarsi di chiudere e disconnettere i propri account del Registro elettronico e/o della piattaforma Gworkspace.**