



ISTITUTO COMPRENSIVO STATALE "RITA LEVI MONTALCINI"

82018 SAN GIORGIO DEL SANNIO (BN) Via G. Bocchini, 37

☎ Segreteria: 0824.49249 ☎ Dirigente: 0824.49140 - C.F. 92057580620 - C.M. BNIC85700T

DR Campania – Ambito BN-4 – Art. 1, c.66, L.13 luglio 2015, n. 107

Decreto USR Campania – Prot. 3988 del 15/03/2016

e-mail : bnic85700t@istruzione.it - sito web : www.icsangiorgiodelsannio.edu.it - P.E.C. : bnic85700t@pec.istruzione.it

Circolare n. 44
Prot. n° 4652/A28

San Giorgio del Sannio, 29/11/2019

- A tutto il personale Docente delle Scuole
 - ✓ Primarie
 - ✓ Infanzia
 - ✓ Secondaria di 1° Grado

- A tutto il personale A.T.A.
Loro sedi

- Al sito WEB dell'Istituto :
www.icsangiorgiodelsannio.edu.it

- Agli Atti della scuola

Oggetto : Dispositivo di pubblicazione Regolamento sull'uso degli strumenti informatici

IL DIRIGENTE SCOLASTICO

- **VISTA** la normativa vigente in materia di utilizzo degli strumenti informatici;
- **VISTO** il proprio Regolamento sull'uso degli strumenti informatici prot. n. 4641/A28 del 28/11/19;

DISPONE

quanto segue :

1. la pubblicazione del Regolamento di cui innanzi, sul sito web dell'Istituzione Scolastica;
2. tutto il personale in indirizzo è tenuto ad osservare il Regolamento;
3. tutto il personale in indirizzo è tenuto a firmare, per accettazione del Regolamento, presso gli uffici di segreteria, dal lunedì al venerdì in orario di apertura al pubblico.



IL DIRIGENTE SCOLASTICO

F.to Prof.ssa Anna POLITO

(Firma autografa sostituita a mezzo stampa ai sensi dell'art. 3, co. 2, DL.vo 39/1993)



ISTITUTO COMPRENSIVO STATALE "RITA LEVI MONTALCINI"

82018 SAN GIORGIO DEL SANNIO (BN) Via G. Bocchini, 37

☎ Segreteria: 0824.49249 ☎ Dirigente: 0824.49140 - C.F. 92057580620 - C.M. BNIC85700T

DR Campania – Ambito BN-4 – Art. 1, c.66, L.13 luglio 2015, n. 107

Decreto USR Campania – Prot. 3988 del 15/03/2016

e-mail : bnic85700t@istruzione.it - sito web : www.icsangiorgiodelsannio.edu.it - P.E.C. : bnic85700t@pec.istruzione.it

Prot. n.4641/A28

San Giorgio del Sannio, 28/11/2019

REGOLAMENTO SULL'USO DEGLI STRUMENTI INFORMATICI

Provvedimenti principali in tema di strumenti informatici:

- 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».

1. Tutti gli strumenti utilizzati dal lavoratore, quali PC, notebook, tablet, smartphone, e-mail ed altri strumenti (di seguito più semplicemente "strumenti informatici"), sono messi a disposizione dall'Ente unicamente per svolgere la propria attività lavorativa.
2. Nell'utilizzare gli strumenti informatici messi a disposizione, il dipendente è tenuto ad usare la massima diligenza, nel rispetto degli obblighi di cui agli articoli 2104 e 2105 del codice civile, utilizzandoli esclusivamente per ragioni di servizio.
3. Comportamenti difforni possono causare gravi rischi alla sicurezza ed all'integrità dei sistemi dell'Ente e possono essere oggetto di valutazione da un punto di vista disciplinare oltre che da un punto di vista penale.
4. Non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori.
5. 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.
6. Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita dell'amministratore di sistema e/o del preposto, in quanto sussiste il grave pericolo di portare virus e di creare rischi seri per la sicurezza informatica.
7. 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'Ente a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software.
8. Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita dell'amministratore di sistema e/o del preposto. Il personal

- computer, inoltre, deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio.
9. Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc...), se non con l'autorizzazione espressa dell'amministratore di sistema e/o del preposto.
 10. L'accesso agli strumenti è protetto da password: si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza.
 11. I log relativi all'utilizzo di strumenti, reperibili nella memoria degli Strumenti stessi ovvero sui server o sui router, nonché i file con essi trattati sono registrati e possono essere oggetto di controllo da parte del titolare del trattamento per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio.
 12. La casella di posta, assegnata dall'Ente all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
 13. 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.
 14. È obbligatorio controllare i file allegati di posta elettronica prima del loro utilizzo. In particolare, si deve evitare, secondo le regole di buona diligenza, l'apertura e la lettura di messaggi di posta elettronica in arrivo provenienti da mittenti di cui non si conosce con certezza l'identità.
 15. Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali particolari è obbligatorio che questi allegati vengano preventivamente resi illeggibili attraverso la crittografia con apposito software (archiviazione e compressione con password). La password di cifratura deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e mai assieme ai dati criptati. Tutte le informazioni, i dati personali e/o sensibili di competenza possono essere inviati soltanto a destinatari – persone o Enti – qualificati e competenti.
 16. Non è consentito l'invio automatico di e-mail all'indirizzo e-mail privato (attivando per esempio un "inoltro" automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, occorrerà prevedere l'utilizzazione di un messaggio "Out of Office" facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di mail alternativo preferibilmente di tipo collettivo.
 17. In caso di cessazione del rapporto lavorativo, la mail affidata all'incaricato verrà disattivata immediatamente. Il sistema in ogni caso genererà una risposta automatica al mittente, informando che la casella di posta elettronica è stata disattivata.
 18. Tutte le informazioni eventualmente raccolte saranno utilizzate per fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 2016/679.

IL TITOLARE DEL TRATTAMENTO

Prof.ssa Anna POLITO



IL RESPONSABILE DEL TRATTAMENTO

Rag. Alfredo CERULO