



ISTITUTO COMPRENSIVO STATALE *Giovanni Falcone e Paolo Borsellino*



Via delle Scuole, 14 - 58023 Gavorrano (GR)

Tel: 0566.844265 – Fax: 0566.846721 - E-mail: gric81800e@istruzione.it - Pec: gric81800e@pec.istruzione.it

C.F.: 80011300532 - C.M.: GRIC81800E

www.icgavorranoscarlino.edu.it

Informativa privacy – lavoro agile/lavoro da remoto

1. Misure di sicurezza per la protezione dei dati personali, ai sensi del GDPR 679/2016

MISURE DI SICUREZZA DA RISPETTARE NELL'UTILIZZO DELLA STRUMENTAZIONE INFORMATICA

Nell'utilizzo della strumentazione informatica bisogna rispettare le seguenti misure:

- lavorare i file direttamente su piattaforma, accedendovi con password dedicata;
- in caso di lavorazione non effettuabile da piattaforma, rimuovere gli eventuali file elaborati presenti sul proprio computer una volta terminata la lavorazione e la finalità per cui il file è stato lavorato;
- in caso di file non terminato durante la sessione, proteggerlo con password dedicata.

Inoltre, il lavoratore impegnato nel lavoro agile dovrà applicare le regole di sicurezza normalmente adottate dall'istituto anche sul proprio pc, che riguardano:

- non lasciare il pc acceso con file con dati personali in visione;
- assicurarsi che quando si trattino dati personali non vi siano persone nelle immediate vicinanze;
- dotare il proprio pc di antivirus;
- le password di accesso devono essere conosciute solo dal soggetto autorizzato;
- password con lunghezza minima di 8 caratteri, sia numerici che alfabetici (o, se il programma in uso non lo permette, dal numero massimo di caratteri consentito);
- password non facilmente riconducibile all'utilizzatore;
- password modificata al primo utilizzo e ogni volta che viene richiesto dal sistema (al massimo ogni 6 mesi) o comunque, nel caso vi sia il dubbio che la stessa abbia perso il carattere di segretezza;
- password segreta con misure cautelative (ad esempio: evitare la digitazione in presenza di terzi, evitare password troppo semplici, non comunicarla a terzi, conservarla in luogo non accessibile a terzi);
- è sconsigliato l'utilizzo di usb a causa della facilità di perdita, furto, diffusione;
- lo stesso vale per gli indirizzi di posta elettronica non istituzionali, più facilmente hackerabili in assenza di idonee password;
- le comunicazioni contenenti i dati degli studenti o del personale ad Enti, associazioni (quali ASL, Regione, ecc.) dovrebbero avvenire esclusivamente via PEC; non utilizzare la propria mail personale;
- non effettuare backup personali dei dati dell'Istituto scolastico sul proprio pc;

- evitare copia/stampe di documentazione sia in digitale che in cartaceo contenente dati personali, presso il proprio domicilio, il cui titolare è l'istituto scolastico;
- qualora si rendano necessarie copie cartacee, l'autorizzato deve implementare tutte le segregazioni fisiche necessarie (es. armadi chiusi a chiave, cassaforte);
- nel caso in cui le copie contenenti il lavoro svolto vengano gettate nel cestino domestico strapparle fino a rendere non ricostruibile il contenuto (effetto distruggi documenti);
- se sono necessarie le copie fotostatiche del lavoro svolto farne in un numero minimo e strettamente necessario;
- stampare e affiggere in corrispondenza della propria postazione di lavoro a casa, lo schema di seguito riportato che contiene le misure di sicurezza minime da rispettare per la protezione dei dati personali.

Smart working: il vademecum per lavorare online in sicurezza

