**MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA**
**ISTITUTO COMPRENSIVO DEL PO**
Via Bonazzi, 9_ 46035 OSTIGLIA (MN) _
TEL 0386/802030 - FAX 0386/802086
e-mail: eduinfo@icdelpo.edu.it - sito web: www.icdelpo.edu.it
Codice IPA: istsc_mnic820005 - Codice Univoco Ufficio: UF0G04
CF: 93034950209 - CM: MNIC820005

**Al DSGA ed Assistenti Amministrativi IC del Po**
**al Collaboratore del Dirigente Scolastico**

# *Circolare interna n.62*

**Oggetto: Istruzioni operative per lo svolgimento del lavoro a distanza.**

In questo momento di emergenza sanitaria si rende necessario disciplinare le norme riguardo l'utilizzo di piattaforme per lo svolgimento di attività lavorativa in remoto.
L'attività di lavoro a distanza svolta tramite ad es. programmi come TeamViewer o simil,i ed effettuata con un pc di proprietà della scuola, ha un impatto limitato sulla sicurezza in materia di privacy.
Tuttavia, poiché si rende necessario anche l'utilizzo di device personali, è opportuno ricordare il rispetto delle misure minime di sicurezza.
Si trasmettono pertanto le istruzioni operative da seguire lo svolgimento dell'attività amministrativa in tutta sicurezza e nel rispetto della normativa vigente in tema di protezione dei dati.
Si ricorda che il trattamento dati dovrà avvenire secondo criteri di liceità, correttezza e trasparenza, accedendo esclusivamente alle banche dati e ai dati personali necessari e pertinenti allo svolgimento dei compiti che sono stati affidati e solo per scopi determinati e legittimi, non eccedenti le mansioni, secondo il principio della minimizzazione dei dati).

**Connessione dati**.
Nello svolgimento dell'attività lavorativa non si devono utilizzare hot spot pubblici gratuiti, come quelli messi a disposizione, ad esempio, da Enti, esercizi commerciali, ecc.
Per quanto riguarda l'utilizzare della propria rete domestica, occorre accertarsi che questa sia protetta almeno con un protocollo WP2 e che siano state modificate le password di fabbrica del router impostandone una robusta secondo i criteri già comunicati.
**Dispositivo utilizzato**
Se si utilizza un dispositivo personale occorre utilizzare sempre lo stesso, al fine di evitare la disseminazione indistinta (dati su più dispositivi) dei dati personali oggetto di trattamento; qualora il dispositivo personale sia condiviso a livello familiare, occorre creare un account dedicato, impostando una password secondo i criteri già comunicati, adottare un sistema di oscuramento (cd. screen-saver) dotato di password e, al termine di ogni sessione lavorativa, interrompere il collegamento.

È necessario che il dispositivo utilizzato sia protetto da antivirus e antimalware aggiornati e da almeno un firewall di tipo software. Non si deve utilizzare il dispositivo al di fuori del proprio domicilio.

**Dati**

In linea generale è vietato esportare file contenenti dati in locale, a meno che non sia indispensabile per il corretto svolgimento dell'attività lavorativa. In ogni caso è necessario che, al termine dell'attività lavorativa quotidiana, i file vengano salvati sul server e non ne rimanga copia in locale.

**Accesso in modalità remota**

L'accesso ai server deve avvenire utilizzando il software messo a disposizione.

La password consegnata deve essere mantenute segreta e non accessibile, onde evitare accessi non autorizzati al server, così come non si deve attivare la modalità di salvataggio automatico della stessa.

**Documentazione cartacea**

In linea generale è vietato portare presso il proprio domicilio documenti cartacei contenenti dati personali. Qualora ciò sia strettamente necessario, si dovrà procedere nel modo seguente:

1. evitare di portare il documento in originale, ma farne sempre una copia, che dovrà essere custodita con la massima diligenza per tutta la durata della sessione lavorativa e riposta in un luogo sicuro al termine della stessa;
2. nel caso di trattamento di dati particolari, di dati di minori o di dati giudiziari, gli atti e i documenti contenenti tali dati devono essere conservati in contenitori muniti di serratura, al fine di escludere l'acquisizione degli stessi da parte di persone non autorizzate del trattamento;
3. al termine del trattamento si dovrà provvedere alla distruzione della documentazione utilizzata.

Al fine di poter procedere alla eventuale messa in sicurezza dei dispositivi utilizzati, si chiede al personale in oggetto di compilare la scheda allegata, relativa alle caratteristiche tecniche dei dispositivi personali in uso, che consentirà sia di verificare che i device consentano il rispetto delle misure minime di sicurezza, sia di avere un elenco dei dispostivi autorizzati.

IL DIRIGENTE SCOLASTICO

***Carla Sgarbi***

**CENSIMENTO PERSONAL COMPUTER PERSONALE PER LAVORO A DISTANZA**

Nome e cognome del dipendente ……..

Ruolo……. Area……

| | |
|---|---|
| Nome del dispositivo (rinvenibile dalle proprietà del computer)** | |
| Sistema Operativo installato(specificare)* | |
| Versione applicativo Office installato | |
| Presenza Antivirus | [_] Si [_] No indicare il nome del prodotto:<br>[_] Avast [_] Avira [_] McaFee<br>[_] AVG [_] Altro _____ |
| Firewall | [_] Si [_] No |
| Connettività | [_] Hotspot Rete Mobile<br>[_] ADSL<br>[_] Fibra |

*Ammessi Windows 8 e successivi.

**Aprire il Pannello di controllo. Fare clic su Sistema e sicurezza > Sistema. Nella pagina Visualizza informazioni di base relative al computer, vedere il nome completo del computer nella sezione Impostazioni relative a nome computer, dominio e gruppo di lavoro.