ISTITUTO COMPRENSIVO MANGONE - GRIMALDI
Scuola dell'Infanzia – Scuola Primaria – Scuola Secondaria di 1° Grado ad indirizzo musicale
Via Provinciale s.n.c. Piano Lago 87050 Mangone (CS)
Tel. e Fax 0984/969171 E.Mail csic851003@istruzione.it
Codice Fiscale 99332920786 Cod. Mecc. CSIC851003

Prot. n. 2145 C1c del 26 marzo 2020

AGLI AA.AA

ALLA DSGA

Loro sedi

Al sito web

Oggetto: raccomandazioni per il corretto svolgimento del lavoro in modalità "Smart working**"**

Undici semplici raccomandazioni rivolte ai dipendenti pubblici che hanno adottato la modalità di lavoro agile per aiutarli a utilizzare al meglio e in sicurezza i propri dispositivi personali:

pc, smartphone, tablet.

Le raccomandazioni sono state elaborate dal Cert-PA di AgID, sulla base delle misure minime di sicurezza informatica per le pubbliche amministrazioni fissate dalla **circolare 17 marzo 2017, n. 1.** L'iniziativa nasce per supportare le PA e i lavoratori Pubblici e sostenerli nel contrastare eventuali attacchi informatici con comportamenti responsabili, anche quando utilizzano dotazioni personali

La direttiva n. 1/2020 emanata dal Dipartimento della Funzione Pubblica prevede, infatti, che il dipendente pubblico possa utilizzare propri dispositivi per svolgere la prestazione lavorativa, purchè siano garantiti adeguati livelli di sicurezza e protezione della rete secondo le esigenze e le modalità definite dalle singole pubbliche amministrazioni.

L'iniziativa è stata avviata da AgID anche a seguito degli ultimi provvedimenti governativi che incentivano l'adozione dello Smart working nelle PA per favorire il contenimento del Covid-19.

Le 11 raccomandazioni di AgID per uno Smart working sicuro

- Segui prioritariamente le policy e le raccomandazioni dettate dalla tua Amministrazione
- Utilizza i sistemi operativi per i quali attualmente è garantito il supporto
- Effettua costantemente gli aggiornamenti di sicurezza del tuo sistema operativo
- Assicurati che i software di protezione del tuo sistema operativo (Firewall, Antivirus, ecc) siano abilitati e costantemente aggiornati

- Assicurati che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy emanate dalla tua Amministrazione
- Non installare software proveniente da fonti/repository non ufficiali
- Blocca l'accesso al sistema e/o configura la modalità di blocco automatico quando ti allontani dalla postazione di lavoro
- Non cliccare su link o allegati contenuti in email sospette
- Utilizza l'accesso a connessioni Wi-Fi adeguatamente protette
- Collegati a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui conosci la provenienza (nuovi, già utilizzati, forniti dalla tua Amministrazione)
- Effettua sempre il log-out dai servizi/portali utilizzati dopo che hai concluso la tua sessione lavorativa

IL DIRIGENTE SCOLASTICO

DOTT.SSA MARIELLA CHIAPPETTA