Oggetto: Informativa in materia di "Telelavoro e Smart Working" ai sensi del Reg. UE 679/16 "GDPR in materia di Protezione dei Dati Personali" e della direttiva n. 1/2020 emanata dal Dipartimento della Funzione Pubblica a seguito dei DPCM 1 aprile 2020 in richiamo dei precedenti DCPM restrittivi anti-contagio - "ulteriori misure di contenimento del Coronavirus Covid-19 e sospensione attività didattiche", nonché tutti i DPCM successivi ed i relativi protocolli che hanno modificato ed integrato le misure anti-contagio Covid 19

In applicazione di quanto previsto dal D.P.C.M. del 1 aprile 2020 e della direttiva n. 1/2020 emanata dal Dipartimento della Funzione Pubblica, in seguito all'allarme Coronavirus e alle misure di prevenzione e controllo decise dal Governo per contenere e limitare il diffondersi del virus COVID-19, nonché si richiamano tutti quelli successivamente emanati che hanno modificato ed integrato le misure anti-contagio. Si comunica che i Dirigenti scolastici organizzano le attività necessarie concernenti l'amministrazione, la contabilità, i servizi tecnici e la didattica, avvalendosi prevalentemente (per quanto possibile) della modalità a distanza, secondo le modalità semplificate previste dalla Nota 6 marzo 2020, n. 278.

Si confermano, fino alla data ultima di emergenza sanitaria disposta con DPCM dal Governo, in merito al lavoro agile e all'attività amministrativa, le disposizioni previste risalgono alla iniziale Nota 6 marzo 2020, n. 278 sono:

- Per il personale ATA, si limiterà il servizio alle sole ulteriori prestazioni necessarie non correlate alla presenza di allievi, attraverso turnazioni del personale attivando i contingenti minimi stabiliti nei contratti integrativi di istituto ai sensi della legge 146/90;
- Le attività di consulenza vanno svolte in modalità telefonica o on-line;
- il ricevimento va limitato ai casi indifferibili, autorizzati dal dirigente preposto alla struttura, con le raccomandazioni di cui ai DPCM vigenti.

Al fine di assicurare tale attività di "Telelavoro e Smart Working", difatti la direttiva n. 1/2020 emanata dal Dipartimento della Funzione Pubblica prevede che il dipendente pubblico possa utilizzare propri dispositivi per svolgere la prestazione lavorativa o quelli ottenuti in comodato d'uso dalla scuola, purché siano garantiti adeguati livelli di sicurezza e protezione.

Le raccomandazioni sono le seguenti:

1. Seguire prioritariamente le policy e le raccomandazioni dettate dalla Amministrazione di appartenenza;

2. Utilizzare i sistemi operativi per i quali attualmente è garantito il supporto;

3. Effettuare costantemente gli aggiornamenti di sicurezza del sistema operativo;

4. Assicurarsi che i software di protezione del sistema operativo (Firewall, Antivirus, ecc.) siano abilitati e costantemente aggiornati;

5. Assicurarsi che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy emanate dalla Amministrazione di appartenenza;

6. Non installare software proveniente da fonti/repository non ufficiali;

Via Magno Magnini, 11 - 06127 PERUGIA
Tel. 075/5010600 **Fax** 075/5010746
E-mail pgee00200l@istruzione.it **PEC** pgee00200l@pec.istruzione.it
Codice Fiscale 80002130542 **Codice Meccanografico** PGEE00200L
Cod. Fatturazione UF5IUH

7. Bloccare l'accesso al sistema e/o configurare la modalità di blocco automatico quando vi si allontana dalla postazione di lavoro;

8. Non cliccare su link o allegati contenuti in email sospette;

9. Utilizzare l'accesso a connessioni Wi-Fi adeguatamente protette;

10. Collegarsi a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui si conosce la provenienza (nuovi, già utilizzati, forniti dalla propria Amministrazione);

11. Effettuare sempre il log-out dai servizi/portali utilizzati dopo che si è conclusa la propria sessione lavorativa.

In effetti il dipendente (assistenti amministrativi e/o lavoratore/trice in telelavoro) in smart working è tenuto innanzitutto a:

- custodire con diligenza la documentazione, i dati e le informazioni dell'Amministrazione utilizzati in connessione con la prestazione lavorativa;

- si chiede agli assistenti amministrativi e/o lavoratore/trice in telelavoro o smart working di mantenere tutti gli obblighi di riservatezza quale incaricato/referenti al trattamento dei dati dell'Ente Scuola in conformità al Regolamento UE 679/16, conservazione in sicurezza e mantenimento in segretezza delle password personali di accesso alla piattaforma, custodire in modo protetto e non accessibile a tutti i terminali utilizzati per espletare il telelavoro e che i dati non siano accessibili a persone non autorizzate e non divulgarli, se non per quelle esclusive finalità istituzionale legale all'Ente Scuola che rimane titolare del Trattamento.

In ottemperanza alle disposizioni comunitarie e nazionali nonché di contratto, il dipendente è tenuto alla più assoluta riservatezza sui dati e sulle informazioni in suo possesso e/o disponibili sul sistema informativo e conseguentemente dovrà adottare, in relazione alla particolare modalità della sua prestazione, ogni provvedimento idoneo a garantire tale riservatezza.

Inoltre, nella qualità di "autorizzato" del trattamento dei dati personali, anche presso il proprio luogo di prestazione fuori sede, dovrà osservare tutte le istruzioni e misure tecniche ed organizzative previste.

In particolare, con riferimento alle modalità smart - work, dovrà:

- porre ogni cura per evitare che ai dati possano accedere persone non autorizzate presenti nel luogo di prestazione fuori sede;
- procedere a bloccare l'elaboratore in dotazione in caso di allontanamento dalla postazione di lavoro, anche per un intervallo molto limitato di tempo;
- qualora non si utilizzino dispositivi forniti dal titolare del trattamento si proceda ad installare almeno un buon sistema antivirus ed effettuare un'accurata scansione preventiva;
- evitare l'uso dei social network, o altre applicazioni social facilmente hackerabili;
- evitare di rivelare al telefono informazioni di carattere personale;
- evitare il collegamento a reti non sicure o sulle quali non si abbiano adeguate garanzie;
- alla conclusione della prestazione lavorativa giornaliera conservare e tutelare i documenti eventualmente stampati provvedendo alla loro eventuale distruzione solo una volta rientrato presso la Sua abituale sede di lavoro;

Via Magno Magnini, 11 - 06127 PERUGIA
Tel. 075/5010600 **Fax** 075/5010746
E-mail pgee00200l@istruzione.it **PEC** pgee00200l@pec.istruzione.it
Codice Fiscale 80002130542 **Codice Meccanografico** PGEE00200L
Cod. Fatturazione UF5IUH

- qualora, invece, al termine del lavoro risulti necessario trattenere presso il proprio domicilio materiale cartaceo contenente dati personali, lo stesso dovrà essere riposto in armadi, cassetti o altri contenitori muniti di serratura.

-I dati potranno essere oggetto di trasferimento all'estero nell'utilizzo di piattaforme di ausilio alla didattica (es. Google, Microsoft).

Via Magno Magnini, 11 - 06127 PERUGIA
Tel. 075/5010600 **Fax** 075/5010746
E-mail pgee00200l@istruzione.it **PEC** pgee00200l@pec.istruzione.it
Codice Fiscale 80002130542 **Codice Meccanografico** PGEE00200L
Cod. Fatturazione UF5IUH