Ministero dell'Istruzione, dell'Università e della Ricerca
Ufficio Scolastico Regionale per la Campania
Istituto Comprensivo Statale "G. Pascoli"

Piazza Risorgimento, 2 - 82100 BENEVENTO
Tel. 0824/1909540 - Fax 0824/1909545
(Plesso Via S. Pertini, 2 -- Tel. 0824 1909503 - 1909504)

CODICE MECCANOGRAFICO BNIC86100D - CODICE FISCALE 8000 42 40 620
E-MAIL ORDINARIA ISTITUZIONALE: bnic86100d@istruzione.it - PEC ISTITUZIONALE: bnic86100d@pec.istruzione.it
SITO WEB: www.icpascolibenevento.gov.it

ISTRUZIONI OPERATIVE ED INFORMATIVE SMART WORKING

L'**Istituto Comprensivo Statale "G. Pascoli" di Benevento** ha adottato una procedura interna diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.
Tutte le istruzioni operative sull'utilizzo delle risorse informatiche e telematiche del nostro istituto scolastico ispirate al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, valgono anche in modalità ***Smart Working***.

Lo ***Smart Working*** è **definito dalla Legge 81/2017** quale modalità d'esecuzione del rapporto di lavoro subordinato caratterizzato dall'assenza di vincoli orari o spaziali e da un'organizzazione per fasi, cicli ed obiettivi stabilita mediante **accordo tra dipendente e datore di lavoro**.
Introduce numerosi vantaggi, ma devono essere tenute in conto diverse problematiche, soprattutto nell'ambito della privacy.
Sicuramente aumenta il rischio per il datore di lavoro che i dati, personali ma non solo, di cui esso risulta Titolare, vengano trattati "in remoto" dal lavoratore non rispettando tutte quelle misure organizzative e/o tecniche messe in piedi dal datore di lavoro per garantire la liceità e la correttezza stessa del trattamento.
Tuttavia, anche il lavoratore vede aumentato il rischio di un ingresso del datore di lavoro nella propria vita personale, se non addirittura in ambienti e luoghi strettamente privati come l'abitazione.
Per quanto riguarda il secondo punto, il datore di lavoro dovrà essere in grado di dimostrare come le tecnologie informatiche non vengano utilizzate esclusivamente per il controllo dell'attività del lavoratore, tutelando la privacy del lavoratore.
Per quanto riguarda il primo punto, molto spesso presso il domicilio del lavoratore, utilizzando dispositivi personali e non forniti dal datore di lavoro, si tende a trascurare le misure di sicurezza che andrebbero adottate: sistemi antivirus/antimalaware, si sottovalutano i piccoli rischi normalmente connessi alla navigazione in rete. Nel caso di utilizzo di sistemi personali, essi dovrebbero per lo meno essere "dedicati" al lavoro installando dei buoni sistemi di protezione (antivirus, firewall, ecc.).
Per la sicurezza informatica, sarebbe opportuno che il datore di lavoro fornisse dispositivi opportunamente configurati e protetti.
In contesti esterni o in occasione di trasferte o di lavoro in mobilità dovranno essere aggiornate e rispettate le policy (IT e posta elettronica o telefono aziendale). Al riguardo, alcune semplici accortezze:

- **evitare l'uso dei social network**, o altre applicazioni social facilmente hackerabili;
- **evitare di rivelare al telefono in presenza di estranei informazioni riguardanti dati personali**;
- **evitare il collegamento a reti non sicure** o sulle quali non si abbiano adeguate garanzie;
- **non lasciare dispositivi o incartamenti incustoditi**.

Dal punto di vista della protezione dati personali, lo smart working implica il coinvolgimento di tutta l'organizzazione e comporta una maggiore responsabilizzazione *(accountability)* dei lavoratori/autorizzati caratterizzati da maggiore autonomia.

L'autorizzato, nella fattispecie, deve salvaguardare i dati personali.

L'istituzione scolastica è chiamata a rendere accessibile al lavoratore una serie di informazioni e documenti necessari all'esecuzione delle proprie mansioni, rimanendo al contempo onerata della protezione degli stessi, quindi del dovere di adottare misure idonee a prevenirne la perdita e/o la diffusione.

Il download o la copia di documentazione sui devices o la possibilità per lo Smart Worker di connettersi a reti pubbliche, non adeguatamente protette, comprometterebbe le esigenze di Protezione dei dati.

Le istituzioni scolastiche dovrebbero adottare, come accade per altre realtà aziendali, una VPN (Virtual Private Network), ovvero una rete privata virtuale che permette, mediante un client, di connettersi ad esempio al server di una organizzazione e lavorare come se si fosse in sede, e di eseguire l'elaborazione di file ed il salvataggio degli stessi in tempo reale direttamente sul server aziendale, oppure da soluzioni in Cloud, di norma un server web sul quale vengono immagazzinati dati, accessibili on demand, che possono quindi essere elaborati, trasmessi ed archiviati.

In un'ottica di protezione dei dati si è diffuso anche il ricorso alle cosiddette ACL (Access Control List), ossia liste di regole che controllano gli accessi ad un sistema informatico, stabilendo quali utenti possono accedere, a quali file o directory e quali azioni siano consentite. Le ACL presentano il vantaggio, anche nella sfortunata ipotesi di intrusioni di soggetti terzi, di non rendere accessibile l'intera documentazione dell'organizzazione, ma solo i file specificamente autorizzati. Inoltre, mediante ACL, è possibile limitare il rischio della perdita di dati ad esempio vietando alcuni tipi di azioni, quali la cancellazione o la copia di documenti.

Il titolare del trattamento
(Istituto Comprensivo "G. Pascoli" nella

figura del suo Rappresentante Legale,
il D.S. Prof.ssa PASSARIELLO Rosetta)

Documento firmato digitalmente
ai sensi del D.Lgs. 82/2005 e s.m.i.