POLICY
SMART WORKING

COD. C.14
VERS. 02 del 02.2026

CONTIENE:

1. **POLICY**

INDICE DELLE VERSIONI SUCCESSIVE ALLA PRIMA:

COD. VERSIONE	DATA MODIFICA	MODIFICHE
02	**02.2026**	**AGGIORNAMENTO A NUOVO CCNL**

PREMESSA

Lo smartworking, inteso come lavoro agile, ha indubbiamente conosciuto l'apice di notorietà durante la pandemia, quando miliardi di persone in tutto il mondo sono state costrette a casa, non potendo, il mondo del lavoro, fare altro che

adattarsi a questo nuovo scenario.
Il nuovo CCNL per il comparto dell'Istruzione e della ricerca, relativo al periodo 2019-2021 introduce la regolamentazione del lavoro distanza per il personale tecnico e amministrativo delle istituzioni scolastiche ed educative (artt. 10, 11 e 12), compatibilmente con le attività svolte nonché con le esigenze e l'organizzazione del lavoro.

Al riguardo si individuano due forme di lavoro a distanza:

- il lavoro agile di cui alla legge n. 81 del 2017, inteso come modalità di esecuzione del rapporto di lavoro subordinato stabilita mediante accordo tra le parti, anche con forme di organizzazione per fasi, cicli e obiettivi e senza precisi vincoli di orario o di luogo di lavoro;
- il lavoro da remoto che avviene con vincolo di tempo e nel rispetto dei conseguenti obblighi di presenza derivanti dalle disposizioni in materia di orario di lavoro, attraverso una modificazione del luogo di adempimento della prestazione lavorativa che comporta la effettuazione della prestazione in luogo idoneo e diverso dalla sede dell'ufficio al quale il dipendente è assegnato.

PASSAGGI DA SEGUIRE

Avviare un progetto di smartworking significa estendere quello che è il perimetro di sicurezza sino a ricomprendere luoghi solitamente non sicuri. Ma questo come può ritenersi compatibile con gli obblighi in capo al datore in base al GDPR?
Semplicemente al datore sarà chiesto di effettuare valutazioni e fornire indicazioni chiare su come dovrà essere svolto il lavoro anche da casa. In tal senso, il datore in prima istanza dovrà garantire i seguenti passaggi:

1. Valutare il livello di sicurezza
2. Distribuire la presente policy ai collaboratori
3. Redigere l'accordo di smartworking
4. Effettuare formazione

VALUTAZIONE DEL LIVELLO DI SICUREZZA

in merito alla necessaria valutazione del livello di sicurezza informatica, è opportuno ricordare che il lavoro da casa può essere svolto dal dipendente con il proprio device o con il device fornito dalla scuola. Nel primo caso si parla di "BYOD/*bring your own device*", scenario descritto e disciplinato in apposita policy da noi fornita; nel secondo caso, invece, è da supporre che il datore abbia a monte valutato il livello di sicurezza del device e che abbia a tempo debito posto rimedio a eventuali criticità. In particolare, è necessario che il datore abbia valutato la presenza: di un sistema operativo cui è garantita la sussistenza di aggiornamenti dalla casa madre; di sistemi antivirus; di una connessione sicura ai database scolastici (es: VPN o cloud), etc.
Una volta esaminati tali parametri, per il datore sarà opportuno evidenziare eventuali attività di rimedio volte a ridurre la distanza tra la situazione riscontrata nel concreto e quella che dovrebbe essere la situazione ottimale.

L'ACCORDO DI SMARTWORKING

L'art. 21 della legge sul lavoro agile (L. 81/2017) stabilisce l'obbligo di stipula di un accordo che disciplini l'esercizio del potere di controllo del datore di lavoro sulla prestazione resa dal lavoratore all'esterno dei locali aziendali nel rispetto di quanto disposto dall'articolo 4 dello Statuto dei lavoratori. Tale accordo deve contenere elementi precisi:

- MODALITÀ ESECUZIONE
- MODI DI ESERCIZIO DEL POTERE DIRETTIVO
- STRUMENTI DI LAVORO UTILIZZABILI
- TEMPI DI RIPOSO
- DIRITTO DI DISCONNESSIONE
- MISURE SICUREZZA

MODALITÀ DI ESECUZIONE

Al collaboratore della scuola, destinatario della presente policy si comunica che, nel caso in cui la prestazione lavorativa

si svolga in smartworking, è comunque necessario individuare un luogo idoneo alla stessa. Non è quindi consentito lavorare da luoghi inidonei quali: palestra, piscina, parchi, luoghi affollati, stadi e, in generale, da tutti quei luoghi che, per loro natura, non permettono di garantire la riservatezza dei dati e la sicurezza dei device utilizzati.

STRUMENTI DI LAVORO UTILIZZATI

Il lavoratore potrebbe utilizzare strumenti propri o strumenti forniti dalla scuola. Nel caso di utilizzo di strumenti propri il collaboratore è tenuto a rispettare la policy in materia di BYOD del Sistema di Gestione EUservice mentre, in caso di strumenti scolastici, il lavoratore è tenuto a utilizzarli correttamente, con la diligenza del buon padre di famiglia, senza quindi arrecare danno, anche involontariamente, agli stessi e garantendo l'impossibilità di accesso e di utilizzo da parte di terzi, familiari compresi.

TEMPI DI RIPOSO E DIRITTO ALLA DICONNESSIONE

In primo luogo, è opportuno ricordare che, anche in smartworking, vige il limite orario massimo giornaliero previsto dal CCNL di settore. Per quanto attiene alle pause, è necessario richiedere all'RSPP di precisare quali e quante pause sono riconosciute al collaboratore in base alle relative previsioni di legge e di contratto collettivo. Da ultimo, si ricorda che il lavoratore, in base alla legge sul lavoro agile, gode del diritto alla disconnessione, vale a dire il diritto a spegnere i propri device e rendersi irraggiungibile al momento della fine dell'orario lavorativo. Simile prescrizione conosce deroga nel solo caso di effettiva emergenza come, ad esempio, nel caso di necessità di attuare un nuovo protocollo emergenziale o nel caso di modificare il proprio orario di lavoro per motivi sopravvenuti e non prevedibili.

GESTIONE DELLE CONFERENCE CALL

In caso di ricorso al lavoro agile è facile che il lavoratore si trovi a dover comunicare con colleghi e studenti per il tramite di cosiddette "conference call". In questo caso, al lavoratore è richiesto di seguire pedissequamente le seguenti istruzioni:

- Assicurarsi che tutte le riunioni siano protette da password, chiedendo ai partecipanti di astenersi dalla condivisione del link a terzi
- Consigliare agli utenti di utilizzare consapevolmente le funzioni di chat, audio, videocamera e condivisione dello schermo
- In caso di condivisione dello schermo, è necessario fare attenzione ed evitare che e-mail o chat siano visibili durante le riunioni
- Quando si usano i video, gli utenti devono assicurarsi che il loro background sia neutro e non riveli alcun dato personale dei loro o altre informazioni riservate
- Optare per un sistema che consenta la gestione centralizzata della conference call, in modo da permettere all'insegnante, tra l'altro, di limitare gli ingressi alla classe virtuale
- Verificare che l'app non invii dati a terzi per scopi pubblicitari o per profilazione
- Consultare il proprio DPO
- Limitare se possibile l'uso della applicazione da dispositivi personali e/o per fini personali
- Assicurarsi che vengano utilizzate solo le distribuzioni ufficiali del programma, aggiornandolo sempre alla ultima versione disponibile
- Identificare i partecipanti alla riunione attraverso l'effettuazione dell'appello e/o dell'accensione delle webcam almeno in fase iniziale

Da ultimo si ricorda di non fornire a terzi le credenziali di accesso ai propri servizi di conference call

ULTERIORI ISTRUZIONI

Al fine di tutelare la sicurezza dei dati dei minori in possesso dell'Istituto Scolastico, il lavoratore è tenuto a rispettare le seguenti indicazioni in materia di privacy:

1. **Utilizzo delle credenziali di accesso VPN:**
   a) Le credenziali di accesso VPN fornite dall'Istituto sono personali e riservate
   b) Inserire manualmente la password di accesso della VPN al desktop remoto ad ogni singolo accesso
   c) Divieto di memorizzare la password VPN di accesso
2. **Protezione del PC personale:**
   a) Dotare il proprio pc di password di accesso
   b) Dotare il proprio pc di dispositivo antivirus
   c) Non aprire e-mail sospette, sia nella casella di posta elettronica d'Istituto sia personali, con oggetto non ben specificato o con richiesta di inserire credenziali di accesso online
   d) Divieto di salvataggio di file di proprietà dell'Istituto sul PC personale o su chiavette USB personali
   e) Evitare di connettersi a siti internet non sicuri
   f) Rispettare la buona abitudine di bloccare l'accesso al PC in caso di allontanamento dalla postazione di lavoro
   g) Spegnere il PC al termine dell'attività lavorativa o al termine della configurazione degli aggiornamenti di sistema
3. **Riservatezza dei dati:**
   a) Il lavoratore è tenuto alla più assoluta riservatezza sui dati e sulle informazioni dell'Istituto in suo possesso
   b) Proibire/evitare l'accesso ai dati/informazioni dell'Istituto Scolastico a persone non autorizzate presso l'abitazione
   c) Conservare adeguatamente eventuali stampe dei documenti dell'Istituto