MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITA' E DELLA RICERCA
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
ISTITUTO COMPRENSIVO ANZIO III
Via Machiavelli s.n.c. tel.06/9873212 - Fax 06/9873540 – rmic8c700e@istruzione.it
00040 Lavinio di ANZIO - ROMA
C.M. RMIC8C700E C.F. 90000150582

LAVORO AGILE E PROTEZIONE DEI DATI PERSONALE

Istruzione operative

Vista la Circolare n. 1/2020 del 04/03/2020 ("Misure incentivanti per il ricorso a modalità flessibili di svolgimento della prestazione lavorativa") emanata dal Ministro per la Pubblica Amministrazione, nella quale si dispone il ricorso in via prioritaria alle modalità di "lavoro agile" o "smart working" nel contesto delle misure di contenimento dell'emergenza epidemiologica da Covid-19, trasmettiamo di seguito le indicazioni operative per il trattamento di dati personali effettuato con queste modalità di svolgimento della prestazione lavorativa. Il presente documento integra quanto già previsto nell'atto di designazione a soggetto autorizzato al trattamento, predisposta dall'Istituto e pubblicata nel sito istituzione alla sezione Privacy, ai sensi dell'art. 29 del RGPD ("Regolamento Generale sulla Protezione dei Dati").

Le indicazioni che seguono sono da considerarsi valide in qualunque condizione di lavoro agile o smart working o lavoro a distanza, sia nella condizione di emergenza attuale, che in contesti di operativirà ordinaria.

Qualunque implementazione dello "smart working", avendo necessariamente a che fare con dispositivi informatici, è necessario che il lavoratore garantisca un adeguato livello di protezione di tali dispositivi, con particolare riguardo al rispetto dei principi di integrità, riservatezza e disponibilità dei dati, al fine di ridurre al minimo i rischi di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità oppure di distruzione o perdita dei dati stessi.

A tale scopo occorre:

1. proteggere l'accesso ai dispositivi informatici (computer, tablet, smartphone) e delle connessioni (cablate o Wi-Fi) attraverso l'uso di password sufficientemente robuste (utilizzare password lunghe, prive di riferimenti ai dati anagrafici propri o dei familiari); sia per l'accesso ai propri dispositivi quanto per l'accesso a Internet. E' prassi diffusa non modificare la password di default per l'accesso alla rete Wi-Fi, una delle principali cause di accessi non autorizzati alla rete locale e, di conseguenza, a tutti i dati e le informazioni in essa contenuti;
2. prediligere, ove possibile, l'utilizzo di sistemi di autenticazione a due fattori (configurabile per gli account dei principali fornitori si servizi di accesso a Internet come Google, Apple, Samsung, Huawei, ecc.);
3. mantenere aggiornati sistemi operativi e software, sia desktop che mobile, utilizzati per svolgere la prestazione lavorativa: gli aggiornamenti sono importanti in quanto spesso risolvono falle di sicurezza sfruttabili per accedere ai dispositivi e ai dati in essi contenuti;
4. implementare sistemi di backup per assicurare la disponibilità di dati ed informazioni in ogni momento, sia tramite sistemi cloud che tramite dispositivi di archiviazione di massa come hard disk portatili e chiavette USB: in entrambi i casi l'accesso ai dati va protetto adeguatamente con soluzioni crittografiche, per rendere i dati inutilizzabili in caso di furto o smarrimento;
5. nel lavorare da casa avere cura nell'allestire la postazione in lavoro in modo da garantile la riservatezza dei dati trattati durante il lavoro, non condividere le informazioni con gli altri occupanti, effettuare il logoff ogni volta che ci si allontana dalla postazione e non lasciare incustoditi supporti di memorizzazione esterna;

United Nations Educational, Scientific and Cultural Organization
Istituto Comprensivo Anzio III
Member of UNESCO Associated Schools

unicef
SCUOLA AMICA

MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITA' E DELLA RICERCA
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
ISTITUTO COMPRENSIVO ANZIO III
Via Machiavelli s.n.c. tel.06/9873212 - Fax 06/9873540 – rmic8c700e@istruzione.it
00040 Lavinio di ANZIO - ROMA
C.M. RMIC8C700E C.F. 90000150582

6. l'accesso ai dati presenti nei pc o negli archivi digitali dell'Istituto deve essere garantito attraverso connessioni dirette come le VPN (Virtual Private Network, collegamenti crittografati tra postazioni remote attraverso internet) appositamente configurate o tramite sevizi Cloud in cui siano stati preventivamente sincronizzati i documenti di lavoro.

Le indicazioni appena elencate sono da ritenersi minime e relative a qualsiasi tipo di concreta applicazione dello "smart working", sia nel caso di utilizzo di dispositivi personali (situazione prevista dal noto paradigma BYOD - porta con te il tuo dispositivo) quanto nel caso di dispositivi configurati e forniti dall'Istituto.

Il Responsabile della Protezione dei Dati

Ing. Angelo Leone

Il Dirigente Scolastico
(Dott.ssa Maria Teresa D'Orso)

Anzio,19 marzo 2020

MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITA' E DELLA RICERCA
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
ISTITUTO COMPRENSIVO ANZIO III
Via Machiavelli s.n.c. tel.06/9873212 - Fax 06/9873540 – rmic8c700e@istruzione.it
00040 Lavinio di ANZIO - ROMA
C.M. RMIC8C700E C.F. 90000150582

SMART WORKING
ATTO DI AUTORIZZAZIONE E ISTRUZIONI ALL'INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI

Gent.ma/mo
premesso che Lei è dipendente della nostra struttura e che a causa dell'emergenza Coronavirus il Governo ha stabilito con DPCM 23.02.2020 e DPCM 4.03.2020 - anche in assenza dell'accordo individuale - l'attivazione immediata, quale modalità ordinaria, su tutto il territorio nazionale dello Smart Working o lavoro agile (art. 18 L. 81/2017) per tutti i tipi di lavori per cui risulti attuabile, al fine di espletare le Sue prestazioni in linea con la disciplina del GDPR 2016/679 e del D.lgs 101/18, occorre che si attenga al seguente

REGOLAMENTO PRIVACY PER LO SMART WORKING
Le prestazioni contrattuali da Lei svolte comportano il trattamento di dati personali e per questo era già stato investito della nomina di incaricato o autorizzato privacy ai sensi degli artt. 4,29,32 e 39 GDPR 2016/679 con apposita lettera. Della ridetta lettera di incarico privacy preme ricordare l'obbligo di attenersi - nonché alle norme di legge - alle Istruzioni allegate di cui in particolare da adeguare e applicare anche nell'attuale condizione di Smart Worker:
- il dovere di non violare il segreto e la riservatezza delle informazioni trattate;
- il dovere di proteggere i dati contro i rischi di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito;
- il dovere di rispettare e applicare le misure di sicurezza fisiche, informatiche, organizzative, logistiche e procedurali;
- il dovere di rispettare e applicare le regole per l'utilizzo degli strumenti informatici ed elettronici, per l'utilizzo della posta elettronica, di internet e delle app.
Si avverte che prima di compiere qualsiasi attività difforme da quanto sopra richiamato occorre assolutamente rivolgersi al proprio referente gerarchico superiore o al titolare del trattamento o all'amministratore di sistema per ottenere eventuale autorizzazione. Agli stessi soggetti occorre immediatamente comunicare qualsiasi anomalia informativa riscontrata nel sistema oppure verificatasi durante l'attività (il tablet e' caduto ma sembra funzionante, lo screen saver non appare più, ecc...).
Si avverte altresì che nella Sua attuale condizione di Smart Worker ha i seguenti specifici obblighi:
- individuare in casa una stanza o comunque uno spazio deputato per allestire la postazione lavorativa che possa essere utilizzato in modo esclusivo interdicendone l'accesso agli altri familiari, con possibilità di chiusura della porta a chiave, con armadietti dotati di serratura ove riporre la documentazione e/o gli strumenti di lavoro;
- assicurarsi della conformità delle prese elettriche domestiche prima di utilizzarle per alimentare il

dispositivo o i dispositivi in uso;
- assicurarsi che la postazione scelta non possa essere investita da acqua, fuoco, vento, calore eccessivo;
- evitare di lasciare incustodita la postazione e al termine di ogni sessione lavorativa riporre tutto in luogo sicuro;
- utilizzare il dispositivo mobile solo ed esclusivamente per le attività lavorative evitando assolutamente di utilizzarlo per accedere a social network o a qualsiasi sito web o server mail che non appartenga a quelli già preventivamente impostati dall'amministratore di sistema;
- evitare di inserire nel dispositivo aziendale pennette USB o comunque basi dati esterne ed evitare di scaricare applicazioni non autorizzate dall'istituto;
- evitare assolutamente di salvare le password sul browser;
- evitare di comunicare con i colleghi tramite mezzi diversi da quelli indicati dal datore di lavoro;
- evitare di postare ai colleghi le proprie credenziali di accesso;
- evitare di condividere con i colleghi documenti o attività lavorative su piattaforme diverse da quelle ufficialmente in uso ed autorizzate o da quella indicata dal datore di lavoro.

Tutto quanto sopra esposto costituisce attualmente - sebbene suscettibile di modifiche e/o integrazioni - il regolamento data protection che lo Smart Worker e' obbligato ad osservare. Tutti gli obblighi sopradescritti fanno parte integrante della prestazione lavorativa e pertanto dovuti. La presente autorizzazione/istruzione ha efficacia fino a quando non verrà revocata la modalità Smart Working da parte del datore di lavoro.

Anzio, 19 marzo 2020

F.to Il Dirigente Scolastico
Dott.ssa Maria Teresa D'Orso
Firma autografa sostituita a mezzo stampa ai sensi e per gli effetti dell'art.3 c.2 D.Lgs n.39/93