ISTITUTO COMPRENSIVO VELLETRI CENTRO
Viale Oberdan, 1 00049 VELLETRI (RM)
TEL 06/9645021 FAX 06/30194068
e-mail rmic8f9002@istruzione.it rmic8f9002@pec.istruzione.it
C.F. 95036910586 www.icvelletricentro.gov.it

A tutto il personale docente e ATA

LAVORO AGILE E PROTEZIONE DEI DATI

Istruzione operative

Vista la Circolare n. 2/2020 della Presidenza del Consiglio dei Ministri contenente "Indicazioni in materia di contenimento e gestione dell'emergenza epidemiologica da COVID – 19 nelle pubbliche amministrazioni di cui all'art. 1, comma 2 del Decreto Legislativo del 30 Marzo 2001 n. 165;
Visti i DPCM adottati ai sensi dell'art. 3, comma 1, del decreto legge 23 febbraio 2020 , n. 6 in attuazione delle misure di contenimento dell'epidemia da COVID-19 e, in particolare, il DPCM 9 marzo 2020 recante misure per il contenimento del contagio sull'intero territorio nazionale tra le quali la sospensione delle attività didattiche fino a 3 aprile 2020 su tutto il territorio nazionale, il DPCM 11 marzo 2020 recante misure urgenti di contenimento del contagio sull'intero territorio nazione che individua la modalità del lavoro agile come modalità ordinaria di svolgimento della prestazione lavorativa nelle pubbliche amministrazioni, al fine di limitare gli spostamenti per il raggiungimento del posto di lavoro per fermare il propagarsi dell'epidemia;
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.

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 operatività ordinaria.

Per 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 garantire 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;
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.

Velletri, 24/03/20

IL DIRIGENTE SCOLASTICO
(Prof.ssa Antonella ISOPI)
(Firma autografa sostituita a mezzo stampa ai sensi e per gli effetti dell'art. 3, c. 2, D. Lgs. n. 39/1993)