MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA

UFFICIO SCOLASTICO REGIONALE PER IL LAZIO

L I C E O S T A T A L E "FARNESINA"

SEZIONE SCIENTIFICA - SEZIONE MUSICALE

Centrale Via dei Giuochi Istmici, 64 - 00135 ROMA Tel. 0636299595 Fax 0636309457
Succursale Via dei Robilant, 7 - 00135 ROMA Tel. e Fax 0633221715
Succursale Via Gosio, 90 - 00191 ROMA Tel. e Fax 06121124705
Distretto Scolastico 28° - Cod. Fisc. 05723890587 - www.liceofarnesina.gov.it - rmps49000c@istruzione.it

INTEGRAZIONE

Atto di designazione a soggetto autorizzato al trattamento

ai sensi dell'art. 29 del RGPD ("Regolamento Generale sulla Protezione dei Dati").

Ai docenti

Al personale AA

Al DSGA

Ai sensi dell'articolo 87 del decreto legge 17 marzo 2020, n. 18, fino alla cessazione dello stato di emergenza epidemiologica da COVID-2019, "il lavoro agile è la modalità ordinaria di svolgimento della prestazione lavorativa" in tutte le pubbliche amministrazioni.

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.

In 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;

MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA

UFFICIO SCOLASTICO REGIONALE PER IL LAZIO

L I C E O S T A T A L E "FARNESINA"

SEZIONE SCIENTIFICA - SEZIONE MUSICALE

Centrale Via dei Giuochi Istmici, 64 - 00135 ROMA Tel. 0636299595 Fax 0636309457
Succursale Via dei Robilant, 7 - 00135 ROMA Tel. e Fax 0633221715
Succursale Via Gosio, 90 - 00191 ROMA Tel. e Fax 06121124705
Distretto Scolastico 28° - Cod. Fisc. 05723890587 - www.liceofarnesina.gov.it - rmps49000c@istruzione.it

2. prediligere, ove possibile, l'utilizzo di sistemi di autenticazione a due fattori (configurabile per gli account dei principali fornitori di 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.

Il Dirigente Scolastico

Prof.ssa Marina Frettoni

Firma autografa omessa ai sensi dell'art. 3 del D.Lgs. n. 39/1993