



UNIONE EUROPEA

FONDI
STRUTTURALI
EUROPEI

po
2014-2020

PER LA SCUOLA - COMPETENZE E AMBIENTI PER L'APPRENDIMENTO-FESR



ISTITUTO COMPRENSIVO PABLO NERUDA
C.F. 97714290588 C.M. RMIC8GR00L

AOO_UF6KM9 - ISTITUTO COMPRENSIVO PABLO NERUDA
Prot. 0002650/LI del 20/03/2020 17:46:12 I.4 - Archivio



MIUR

Dipartimento per la Programmazione
Direzione Generale per interventi in materia di edilizia
scolastica, per la gestione dei fondi strutturali per
l'istruzione e per l'innovazione digitale
Ufficio IV



MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO

Istituto Comprensivo "Pablo Neruda"
Via Casal del Marmo n. 212 - 00135 Roma

Cod. Fisc. 97714290588

✉ RMIC8GR00L@istruzione.it - Rmic8gr001@pec.istruzione.it

☎ 06/30819741 fax 06/308197

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 operatività 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 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 e di informazioni in ogni momento, sia tramite sistemi cloud che tramite dispositivi di archiviazione di massa come hard disk portatili e



UNIONE EUROPEA

FONDI
STRUTTURALI
EUROPEI

pon
2014-2020

PER LA SCUOLA - COMPETENZE E AMBIENTI PER L'APPRENDIMENTO-FESR



Ministero dell'Istruzione, dell'Università e della Ricerca
Dipartimento per la Programmazione
Direzione Generale per interventi in materia di edilizia
scolastica, per la gestione dei fondi strutturali per
l'Istruzione e per l'innovazione digitale
Ufficio IV

MIUR



MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO

Istituto Comprensivo "Pablo Neruda"

Via Casal del Marmo n. 212 - 00135 Roma

Cod. Fisc. 97714290588

✉ RMIC8GR00L@istruzione.it - Rmic8gr001@pec.istruzione.it

☎ 06/30819741 fax 06/308197

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 servizi 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

Ultima revisione del 03/2020

IL DIRIGENTE SCOLASTICO
PROF.SSA BRUNELLA MARTUCCI