MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA

I.I.S. "E. Mattei" – CASTROVILLARI

Liceo Scientifico e Linguistico - "E-Mattei" – I.T.C.G. "Pitagora-Calvosa"

Test center ECDL

Sede Uffici - Viale delle Querce – 87012 Castrovillari (CS) - Cod.Mecc.: CSIS079003 - Cod. Fisc.: 94032120787

Tel. 0981.1989913 - Fax 0981.491864 (Presidenza e Segreteria) - Tel.Sede ITCG "Pitagora-Calvosa" 0981.21889

www.liceomattei.edu.it - csis079003@istruzione.it – csis079003@pec.istruzione.it

Linee guida specifiche per il personale docente in DDI, DAD e FAD

Misure operative per garantire la sicurezza del trattamento dati GDPR Regolamento UE 679/2016

Le presenti linee guida forniscono le indicazioni operative per il trattamento di dati personali effettuato al di fuori della sede di lavoro, mediante le modalità di svolgimento della prestazione lavorativa a distanza.

Le prescrizioni sottoriportate dovranno essere attese, se possibile, con ancora più attenzione per garantire un livello di protezione adeguato delle dotazioni tecnologiche attraverso le quali svolge le lezioni a distanza e rispettare i principi di integrità, riservatezza e disponibilità dei dati e delle informazioni ivi contenute, 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.

Pertanto, Lei dovrà rispettare le seguenti direttive

1. L'utilizzo delle dotazioni tecnologiche deve avvenire nel rigoroso rispetto delle linee guida e delle istruzioni fornite dall'Amministrazione.
2. Nell'esecuzione della prestazione lavorativa a distanza, il lavoratore è tenuto al rispetto degli obblighi di riservatezza, ai sensi del decreto del Presidente della Repubblica 16 aprile 2013, n. 62, "Regolamento recante codice di comportamento dei dipendenti pubblici" e ss.mm.ii e dell'art. 13 del CCNL del 18/04/2018.
3. Restano ferme le disposizioni in materia di responsabilità, infrazioni e sanzioni contemplate dalle leggi e dai codici di comportamento sopra richiamati, che trovano integrale applicazione anche al lavoratore agile.
4. Riguardo al trattamento dei dati personali, ovviamente anche fuori sede il dipendente dovrà osservare tutte le istruzioni e le misure di sicurezza previste dalla normativa sulla privacy e riportate nelle linee guida allegate.

In particolare, il docente:

- deve porre ogni cura per evitare che ai dati possano accedere persone non autorizzate presenti nel luogo della prestazione lavorativa fuori sede;
- deve rendere inaccessibile a terzi l'elaboratore in dotazione in caso di allontanamento dalla postazione di lavoro, anche per un intervallo limitato di tempo;
- alla conclusione della prestazione lavorativa giornaliera è obbligatorio custodire, conservare e tutelare i documenti eventualmente stampati provvedendo a distruggerli o a portarli in sede una volta terminato il periodo

Principali prescrizioni in tema di sicurezza informatica

1. Proteggere l'accesso alla rete (LAN, WiFi) e alle dotazioni tecnologiche (PC, notebook, tablet, smartphone, ecc.) attraverso l'uso di password forti e diverse per ciascun servizio[1]. Allo scopo si prescrive il cambio delle password utilizzate abitualmente per l'accesso alle varie applicazioni in cloud. Si consiglia, inoltre, il cambio della password di accesso della propria linea ADSL. Laddove possibile, utilizzare l'autenticazione a due fattori. Ad esempio, gli applicativi Argo consentono l'attivazione del PIN di autenticazione in aggiunta alla password d'accesso. Medesima possibilità è garantita dagli account Microsoft.

2. Garantire che i sistemi operativi installati sulle workstation (PC, notebook, tablet, smartphone) siano autentici e aggiornati all'ultima versione disponibile. Non è consentito lo smart working attraverso workstation dotate di sistemi operativi privi del supporto (ad esempio Windows 7) o peggio non autentici (privi della licenza d'uso). Le vulnerabilità proprie dei sistemi operativi non autentici o privi del supporto e quindi non aggiornati con le ultime patch di sicurezza è la prima causa di accesso non autorizzato alla rete e alle informazioni.

3. Nel caso di utilizzo di una workstation condivisa (PC, notebook, tablet) è obbligatorio implementare un nuovo account d'accesso al sistema, personale e riservato.

4. Garantire la presenza, sulla propria workstation, di un firewall e di un sistema antivirus. Il sistema antivirus deve essere sempre attivo e aggiornato in real time (va bene, ad esempio, anche Avira nella sua versione non commerciale). Il firewall (va bene anche quello integrato nel sistema operativo Windows) deve sempre essere attivo e non deve prevedere alcuna eccezione.

5. È assolutamente vietata la pratica di memorizzazione delle password dei vari account nel browser. È consigliabile evitare di memorizzare anche le user name. Pertanto, il completamento automatico deve essere disabilitato. Si consiglia di utilizzare, per l'accesso ai vari account in cloud, sempre lo stesso browser. La memorizzazione degli account in cloud può essere consentita solo in presenza di un gestore di password crittografico (ad esempio, l'applicazione "Password Manager" integrata nella suite gratuita di Avira).

6. Nel caso in cui si proceda a memorizzare in locale qualsivoglia tipologia di informazioni, anche temporaneamente, le stesse non dovranno mai essere memorizzate sull'hard disk della workstation, ma sempre in un dispositivo rimovibile (ad esempio pen drive, hard disk portatile) protetto su base crittografica. A tal proposito è possibile attivare la funzione "Attiva Bitlocker" fornita dal sistema operativo Windows.

[1] La password deve essere sufficientemente lunga e complessa, ad esempio deve essere composta da almeno 8 caratteri, contenere almeno un carattere appartenente alle lettere maiuscole e almeno un carattere appartenente alle lettere minuscole, contenere almeno un carattere appartenente alle 10 cifre (0-9), contenere almeno un carattere appartenente ai caratteri non alfabetici (ad esempio !,$,#,%), essere diversa dall'ultima utilizzata e mai riconducibile alla propria sfera personale o professionale.