POLICY

USO DATI PC LABORATORI E RE (DOMINIO/NON DOMINIO)

COD. C.11

VERS. 01 DEL 05.2022

CONTIENE:

INDICE DELLE VERSIONI SUCCESSIVE ALLA PRIMA:

COD. VERSIONE	DATA MODIFICA	MODIFICHE

PREMESSA

Con la presente policy vengono fornite delle brevi e semplici indicazioni per il corretto trattamento dei dati all'interno dei pc di laboratorio ed in generale di tutti i pc della scuola e del registro elettronico.

DISPOSIZIONI SUL CORRETTO TRATTAMENTO DEI DATI ALL'INTERNO DEI PC DELLA SCUOLA

1. Le credenziali di accesso username e password ai pc della scuola sono personali e riservate. Tutto il personale dell'organizzazione deve capire l'importanza di mantenere le credenziali personali e riservate. Da un punto di vista di *privacy compliance*, la cessione delle proprie credenziali ad altra persona rappresenta sempre potenzialmente una violazione della riservatezza o della disponibilità dei dati contenuti all'interno del profilo dell'interessato.

PARTICOLARI CONSIDERAZIONI
- Si segnala di non cedere mai le proprie credenziali ad altra persona in quanto tale eventualità, in caso di data breach, potrebbe costituire un concorso nella violazione verificatasi - Sebbene per legge il Titolare risulti essere l'unico soggetto ad essere sanzionato non si escludono con il passare del tempo interpretazioni giurisprudenziali che rendano anche l'incaricato sanzionabile

2. La politica del cambio password periodica è una misura di sicurezza organizzativa necessaria al fine di garantire la *privacy compliance* che viene decisa e fatta implementare da parte del Dirigente scolastico sulla base dei requisiti descritti, tra l'altro, nel Sistema di Gestione EUservice

NOTA BENE
- Per quanto il DPO consigli al Dirigente scolastico di adottare il cambio password se tale misura non viene fatta rispettare in maniera ferrea da parte del Dirigente scolastico difficilmente l'organizzazione si atterrà alle indicazioni riportate all'interno delle lettere di incarico del personale autorizzato al trattamento dei dati.

3. Non archiviare dati personali all'interno dei pc di laboratorio i.e. elaborati digitali, allegati mail, elenchi di dati personali, etc.

OSSERVAZIONI
- Il GDPR impone, al fine di ottemperare ai principi declinati nell'art. 5 del Regolamento, di rendere l'accesso ai dati minimo e indispensabile e quindi di garantire le proprietà CIA del dato (confidenzialità, integrità e disponibilità). - Pertanto, i dati vanno conservati all'interno delle reti scelte da parte della scuola (i.e. rete di segreteria, rete didattica, repository etc.) - Questo significa che i dati non vanno conservati in locale. Il salvataggio dei dati in locale può essere effettuato solo provvisoriamente dall'utente, ma poi il dato andrà cancellato dalle relative cartelle in locale, dal desktop e dal cestino. **In caso di attacco informatico o di accessi non autorizzati l'accesso ai dati salvati in locale sarebbe immediato.**

4. Seguire le indicazioni particolari fornite dal Dirigente scolastico evitando per esempio di navigare su siti non sicuri, di aprire profili social personali, controllare la posta elettronica della mail personale non di lavoro etc.

Il Dirigente Scolastico può adattare un mansionario al contesto dell'organizzazione, da allegare inoltre alle lettere di incarico degli autorizzati al trattamento dei dati personali.

5. Ricordarsi di spegnere il pc al termine della sessione di lavoro.

Se vi dimenticate il PC acceso e un altro utente accede con intenzioni malevoli al vostro profilo eventuali *data breach* purtroppo potrebbero essere riconducibili ai vostri accessi.

DISPOSIZIONI SUL CORRETTO TRATTAMENTO DEI DATI ALL'INTERNO DEL REGISTRO ELETTRONICO

1. Non annotare comunicazioni riservate a specifici utenti all'interno dello spazio di dominio pubblico del registro elettronico in quanto questo comportamento può rappresentare una violazione della riservatezza degli interessati.

Anche all'interno del registro elettronico, sebbene sia uno strumento sicuro, non tutti gli utenti che vi accedono devono leggere tutto.

Si ricorda a tal proposito che il Garante ha già irrogato delle sanzioni per errate pubblicazioni all'interno del registro elettronico sebbene il trattamento riguardasse dati personali resi manifestamente pubblici da parte degli interessati.

2. Le credenziali di accesso al Registro Elettronico sono personali e riservate ed in quanto tali esse non vanno cedute a terzi per nessun motivo.

3. Se ci si accorge che qualcuno è entrato all'interno del proprio profilo del registro elettronico e/o registro di classe effettuare immediatamente il cambio password e segnalare **tempestivamente** l'incidente al Dirigente scolastico e al DPO per verificare la gravità della violazione, rispettando le disposizioni di cui alla policy data breach C. 08 di cui al Sistema di Gestione EUservice.

Al termine dell'orario di lezione e/o per qualsiasi motivo di interruzione della lezione con uscita dalla classe ricordarsi di effettuare il LOG OUT dal registro di classe.

IN SINTESI
Non si prestano le credenziali user name e password ad altri utenti.
Non si conservano i dati in locale.
Non si comunica sul registro elettronico senza prestare la dovuta attenzione ai destinatari.
Al termine di ogni sessione, ricordarsi di effettuare il log-out.