



ISTITUTO COMPRENSIVO CHIOGGIA 3
SCUOLA INFANZIA - SCUOLA PRIMARIA – SCUOLA SECONDARIA DI 1° GRADO
Cod. Min. VEIC85000R Cod. Fiscale 91020300272 Distretto Scolastico n.° 56
Presidenza e Segreteria Via P.Togliatti, 831 C.a.p. 30015 CHIOGGIA – VE
Tel. 041/400096 e-mail veic85000r@istruzione.it
P.E.C. veic85000r@pec.istruzione.it

Circolare n. 238

Chioggia, 17.04.2023

A tutti i Docenti

Al personale ATA

Oggetto: Indicazioni operative per la gestione dei dati nella piattaforma didattica Office 365

Visto l'ultimo ammonimento del gruppo MonitoraPA 28 febbraio 2022;

Visto che le piattaforme didattiche esportano i dati in territorio statunitense e che ad oggi lo scudo Privacy Shield non è ancora stato ripristinato;

Visto che il Garante sia nel provvedimento del 26 marzo 2020 n. 9300784 e l'intervento 05 luglio 2020 dell'Avv. Guido Scorza, componente del collegio del Garante Nazionale;

È necessario definire alcune importanti linee operative che hanno il compito di ridurre il rischio di incidenti nel trattamento dati, soprattutto dei dati sensibili. È importante cercare di seguirle in modo più scrupoloso possibile.

1) Utilizzare una password sicura

Una password è sicura, cioè difficile da violare o craccare, se è sufficientemente lunga e complessa. Ad es.: una password di otto caratteri, composta solo da lettere minuscole, può essere potenzialmente violata in meno di un minuto.

Una password è sicura se:

- è composta da almeno 13 caratteri
- contiene non solo lettere minuscole, ma anche lettere maiuscole, numeri e simboli o caratteri speciali (come !, ?, =, etc.)

2) Effettuare sempre il logout quando si utilizzano computer pubblici

Se si utilizza, il proprio account utilizzando un computer pubblico o condiviso (ad es. in aula insegnanti, in aula informatica, usando il notebook presente in classe, etc.) è fondamentale, prima di allontanarsi dal dispositivo, effettuare sempre il **logout**, cioè uscire dal proprio account, per evitare che altri soggetti possano effettuare trattamenti con i dati presenti nello stesso.

3) Usare nelle mail l'azione di linkare i documenti e non allegarli

Per evitare, che tramite l'utilizzo della posta elettronica d'Istituto uno o più documenti vengano inviati a soggetti non autorizzati al loro trattamento, è necessario utilizzare la condivisione del documento dal cloud (onedrive o drive) piuttosto che allegare gli stessi in un messaggio di posta elettronica. In questo modo in caso di errori materiali, sarà possibile, velocemente, chiudere la condivisione ed evitare che il documento venga trattato da soggetti non autorizzati.

4) Gestione di documenti contenenti dati sensibili, sanitari e giudiziari all'interno del cloud

È necessario che i documenti che contengono dati, nello specifico sensibili, sanitari e giudiziari, rimangano depositati nel cloud e quindi gestibili per il tempo necessario, perché il personale scolastico possa elaborarli in team e definire un documento finale che dovrà poi essere archiviato nel

gestionale di segreteria o registro elettronico. La documentazione, in formato bozza o revisione, restante nel cloud dovrà essere cancellata.

5) Pulizia e ordine della propria parte di spazio nel cloud

Per poter applicare uno dei principi fondamentali del GDPR, è il principio di minimizzazione. Per poterlo applicare è necessario tenere ordinato e soprattutto eliminare documentazione, contenente dati sensibili, sanitari e giudiziari che non è più necessaria per svolgere la propria attività lavorativa.



Il Dirigente Scolastico
prof.ssa Sandra Zennaro