



ISTITUTO COMPRENSIVO STATALE

Scuola Infanzia, Primaria e Secondaria I Grado

87010 TERRANOVA DA SIBARI (CS)

Tel. 0981/957354 - FAX 0981/955092 – Via Orto S. Antonio Cod. Fisc.: 94006030780 –

Cod. Mecc.CSIC842008 Sito web: <http://www.ic.terranovadasibari.edu.it/>

Email: csic842008@istruzione.it- Codice Univoco UFL1E5

Terranova da Sibari, 14/04/2020

I. C. S. TERRANOVA DA SIBARI
Prot. 0001047 del 14/04/2020
(Uscita)

Al Personale Docente
Ai Genitori degli alunni di ogni ordine e grado
Al DSGA
Al personale A.T.A.
Dell'Istituto Comprensivo
Terranova da Sibari
SEDI
Al sito web
All'Albo

OGGETTO: Comunicazioni: “Provvedimenti e indicazioni Garante Privacy sulla didattica a distanza”

Con la presente si provvede ad analizzare i provvedimenti e le prime indicazioni fornite Dal Garante Privacy in merito al trattamento dei dati personali degli interessati, relativamente alle attività connesse alla didattica a distanza (DaD). Come già affermato nella precedente comunicazione del 9 marzo u.s., la scuola non deve richiedere alcun consenso agli interessati per lo svolgimento della didattica a distanza, in quanto secondo quanto affermato dall'Autorità, essa è *“riconducibile – nonostante tali modalità innovative – alle funzioni istituzionalmente assegnate a scuole ed atenei”*. **Si comunicano, altresì, le seguenti procedure da attivare/verificare per garantire la conformità al GDPR delle attività connesse alla DaD.**

- Fate in modo che le applicazioni per la videoconferenza siano gestite in un **ambiente riservato** (ad esempio Meet tramite il dominio riservato G Suite), evitando applicazioni per la videoconferenza che mettono a disposizione stanze **“pubbliche”** per le attività. Tanto si rende necessario per garantire che i partecipanti alle attività siano **solo ed esclusivamente gli aventi diritto** ed evitare la presenza di utenze estranee e non autorizzate. In alternativa si rende necessario (laddove possibile) proteggere l'accesso al meeting tramite un codice riservato o altra procedura simile. In ogni caso, deve sempre essere possibile **identificare la presenza** di utenze esterne e non approvate, durante un meeting e più in generale durante qualunque attività riferita alla DaD.
- Accertarsi che gli strumenti individuati per la DaD e specificatamente quelli per le videoconferenze **non adottino sistemi di monitoraggio sistematico degli utenti**. In tal caso è necessario disattivare tale opzione.
- Accertarsi che gli strumenti individuati per la DaD non facciano ricorso alla **geolocalizzazione** o a **sistemi di social login** (accesso alla piattaforma basato, ad esempio, su un account Facebook preesistente). Più in generale è necessario verificare che gli strumenti adottati per la DaD non adottino **tecniche di profilazione dei dati a fini commerciali**.
- Attenzione alle procedure messe a disposizione dagli strumenti per la videoconferenza relative alla **registrazione del meeting**. Tale registrazione (sia da parte dei docenti che degli allievi) è da considerarsi

legittima se **utilizzata a scopi esclusivamente personaliz.** È esclusa qualsiasi forma di diffusione o comunicazione senza il consenso esplicito di tutti gli interessati. Ovviamente, la responsabilità della comunicazione o della diffusione è direttamente relazionata al singolo individuo. Anche la disabilitazione (ove possibile) di tale funzione non risolve alla radice il problema: sarebbe, comunque, possibile e banalmente con altri strumenti registrare il meeting (così come sarebbe possibile durante l'attività in presenza). La soluzione è da ricercarsi nel livello di consapevolezza e responsabilità dell'utenza.

Si segnala, inoltre, che CERT-PA (Computer Emergency Response Team della Pubblica Amministrazione) ha riportato evidenze sull'utilizzo improprio della piattaforma Zoom per veicolare malware e specificatamente nella funzione di chat e nella protezione delle password. Si invitano pertanto le istituzioni scolastiche a valutare l'opportunità di utilizzare la piattaforma Zoom tenuto conto anche delle numerose segnalazioni pervenute su rischi per il trattamento dei dati degli studenti coinvolti. Non ultimo la piattaforma è stata attenzionata anche e non solo sotto il profilo del controllo sul livello dell'attenzione dei partecipanti a meeting o video lezioni.

Si sottolinea infine che: in riferimento all'applicazione Whatsapp utilizzata per lo scambio tra docenti e alunni di compiti assegnati e relative e per lo scambio tra docenti di documentazione riservata riferita al proprio dovere d'ufficio (ad esempio verbali dei consigli di classe), non è conforme alle norme prescritte dal GDPR.

Pertanto si ricorda che:

- Whatsapp è uno strumento di messaggistica **privata**, la cui utenza telefonica è intestata al legittimo proprietario soggetto privato e **non all'istituzione scolastica**, che è **titolare del trattamento**;
- I compiti assegnati e inviati tramite Whatsapp (o applicazioni similari), rimangono **atti privati non documentati e non documentabili e non assurgono ad atti amministrativi**, così come invece si caratterizzano tutti gli atti allocati nel registro elettronico o attraverso le piattaforme istituzionalmente riconosciute.

Se ne deduce e si ribadisce che qualunque procedura, strumento o applicazione utilizzata nella didattica a distanza al di fuori di quanto previsto dalle disposizioni del dirigente, in considerazione di quanto indicato dal Garante della Privacy, non potrà che generare, nel caso di illecito, responsabilità diretta disciplinare, civile e penale.

IL DIRIGENTE SCOLASTICO
Maria Letizia Belmonte
*(Firma autografa sostituita a mezzo stampa
ai sensi dell'art. 3, comma 2, del D.Lgs. 39/93)*