MINISTERO DELL'ISTRUZIONE DELL'UNIVERSITA' E DELLA RICERCA
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
ISTITUTO COMPRENSIVO "ANTONIO DE CURTIS"
Via della Tenuta di Torrenova, 130 - 00133 ROMA
☎062022705 Fax. 0620419196 - cod.mec. RMIC85200L – cod. fisc. 97020470585
www.icdecurtis.edu.it
e-mail: rmic85200l@istruzione.it RMIC85200L@PEC.ISTRUZIONE.IT

Prot. n. 0001810/U
Roma, 20/05/2020

A tutto il personale
Al D.S.G.A.
Sito web

Oggett: Disposizioni privacy e sicurezza dei dati nella didattica a distanza

Si trasmettono in allegato le disposizioni per la tutela della privacy e sicurezza dei dati nella didattica a distanza contenute nel documento elaborato dal DPO d'Istituto.

AUMENTARE LA SICUREZZA

1. Assicurarsi che tutte le riunioni siano protette da password, chiedendo agli alunni di astenersi dalla condivisione del link a terzi. Se possibile, avvisare tutti gli utenti di proteggere il proprio account selezionando password complesse e abilitando l'autenticazione a più fattori.
2. Astenersi dal registrare le lezioni a meno che non sia indispensabile.
3. Consigliare agli utenti di utilizzare consapevolmente le funzioni di chat, audio, videocamera e condivisione dello schermo.
4. In caso di condivisione dello schermo, è necessario fare attenzione ed evitare che e-mail o chat siano visibili durante le riunioni.
5. Quando si usano i video, gli utenti devono assicurarsi che il loro background sia neutro e non riveli alcun dato personale dei loro o altre informazioni riservate.
6. Assicurarsi che la applicazione supporti la comunicazione crittografata tipo end-to-end.
7. Optare per un sistema che consenta la gestione centralizzata della conference call, in modo da permettere all'insegnante, tra l'altro, di limitare gli ingressi alla classe virtuale.
8. Leggere attentamente l'informativa sulla privacy del programma facendo attenzione a: tipi di dati raccolti e memorizzati; possibili trasferimenti di dati verso paesi terzi; periodi di conservazione.
9. Verificare che l'app non invii dati a terzi per scopi pubblicitari o per profilazione.
10. Consultare il proprio DPO.
11. Limitare se possibile l'uso della applicazione da dispositivi personali e/o per fini personali.
12. Assicurarsi che vengano utilizzate solo le distribuzioni ufficiali del programma, aggiornandolo sempre alla ultima versione disponibile.

DISPOSIZIONI PER LA GESTIONE DELLA PIATTAFORMA "ZOOM"

1. **AGGIORNA ZOOM ALLA VERSIONE 5**
2. **NON CONDIVIDERE IL TUO ID**- Ogni account Zoom è dotato di un proprio meeting ID. Condividere questo ID permette a chiunque di introdursi nelle conversazioni in atto. Per questo è meglio optare per la creazione di meeting diversi di volta in volta
3. **CREA LA SALA DI ATTESA** -Predisporre la c.d. sala di attesa, questo permetterà di scegliere chi fare entrare e chi no.
4. **IMPOSTA LA PASSWORD** -Preimpostare sempre una password di accesso ai meeting così da rendere ulteriormente difficoltosa l'intrusione di soggetti non autorizzati.
5. **BLOCCA NUOVI INGRESSI** - Una volta iniziata la lezione si suggerisce di utilizzare la funzione Lock Meeting: questa opzione permette di bloccare l'accesso di nuovi (e non autorizzati) partecipanti alla riunione.

POLICY PER IL PERSONALE

1. Assicurati di accedere al sistema operativo con un account riservato all'attività lavorativa e dotato di password sicura.
2. Utilizza sistemi operativi per i quali è garantito il supporto ed effettua costantemente gli aggiornamenti.
3. Assicurati che i software antivirus siano abilitati e costantemente aggiornati.
4. Non installare software provenienti da fonti non ufficiali.
5. Non cliccare su link o allegati contenuti in email sospette.
6. Utilizza l'accesso a connessioni Wi-Fi protette.
7. Collegati a dispositivi mobili (es. pen drive e hard disk esterni) di cui conosci la provenienza.
8. Allestisci la postazione di lavoro in modo da garantire la riservatezza dei dati ed effettua il log-out dai servizi/portali utilizzati dopo che hai concluso la sessione lavorativa.
9. Implementa sistemi di backup, prediligendo servizi cloud o dispositivi di archiviazione cifrati (es. pen drive e hard disk esterni).
10. L'accesso ai dati da remoto deve avvenire tramite VPN o tramite servizi Cloud qualificati dall'AgID.

Si ricorda che i dati di contatto del DPO sono disponibili alla pagina PRIVACY del sito web dell'Istiuto.

Il Dirigente Scolastico
Prof.ssa Serafina Di Salvatore
(Firma autografa sostituita a mezzo stampa ex art.3, c2D.L.gs n. 39/93)