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

Roma, 8/06/2020

Ai genitori
Agli alunni
Ai docenti
Sito web

Oggetto: Regolamento presentazione orale degli elaborati

In vista dell'imminente chiusura dell'anno scolastico e della presentazione orale degli elaborati inviati dagli alunni , si ritiene opportuno ricordare quanto già precedentemente disposto con varie circolari rispetto agli obblighi di comportamento per quanti si avvalgano delle modalità di didattica in videoconferenza.

ALUNNI

Durante il collegamento in videoconferenza gli alunni sono invitati a rispettare le seguenti indicazioni:

- collegarsi puntualmente cinque minuti prima dell'orario previsto per la videoconferenza per evitare che l'ingresso nella classe virtuale disturbi la presentazione in corso
- avere la telecamera accesa all'inizio del collegamento e per tutta la sua durata per essere identificati dai docenti;
- inserire il proprio cognome e nome (non diminutivo, non nickname, o altro) per essere riconosciuto durante tutta la durata della videoconferenza;
- avere un comportamento corretto nell'aula "virtuale" e un abbigliamento consono alla situazione;
- essere (se possibile) in un luogo tranquillo, a tutela di sé e dei compagni di classe, eccetto situazioni particolari che vanno comunicate al docente all'inizio della lezione;
- non «aprire» la partecipazione alle videoconferenze a soggetti terzi;
- non fare foto o riproduzioni; **eventuali foto o riproduzioni NON possono essere diffuse**;
- non diffondere le credenziali di accesso e/o il link delle videoconferenze, essendo queste rigorosamente personali.

DOCENTI

Si rimanda a quanto comunicato nella nota prot. n. 0001810/U del 20/05/2020 relativamente alle disposizioni per la tutela della privacy e sicurezza dei dati nella didattica a distanza, contenute nel documento elaborato dal DPO d'Istituto, e che si ritiene opportuno riportare di seguito:

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.

Si raccomanda il puntuale rispetto di quanto

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.

FAMIGLIE

In riferimento alle attività didattiche e alle presentazioni orali dell'elaborato in videoconferenza, si ricorda che le immagini ivi riprodotte hanno una finalità strettamente didattica e istituzionale.

Pertanto, si informano i Sigg,ri Genitori/tutori legali di quanto segue:

- le videoconferenze hanno finalità didattiche/istituzionali e sono monitorate dai docenti;
- le credenziali di accesso saranno comunicate direttamente alla famiglia dell'alunno;
- le regole d'uso della piattaforma e per l'accesso al dominio sono presenti sul sito della piattaforma utilizzata;
- è obbligatorio rispettare le disposizioni previste dal del GDPR n. 679 del 2016, del Codice della Privacy, così come adeguato e modificato, con D.LGS. n. 101 del 2018.

Si ricorda che ai sensi della normativa vigente è assolutamente vietato registrare in qualsiasi modo e tramite qualsiasi strumento le videoconferenze tenute dai docenti. E' inoltre vietato registrare, conservare e diffondere con qualsiasi mezzo e per qualsiasi scopo immagini fisse, sequenze video e sequenze audio contenenti immagini o voci di terzi, senza il previo consenso scritto di questi ultimi. Gli alunni durante le videoconferenze si trovano sotto la responsabilità dei genitori e dunque ai sensi dell'art.2048 Codice civile, i genitori sono responsabili di illeciti che dovessero verificarsi in merito alle registrazioni e alle diffusioni delle videoconferenze , che si ribadisce sono vietate.

Chiunque, in spregio a quanto sopra, non si attenga alle presenti disposizioni sarà responsabile personalmente delle violazioni di cui all'art. 10 c.c, nonché di un'eventuale diffusione pubblica o comunicazione a terzi del medesimo materiale, ovvero, del trattamento illecito di dati di cui all'articolo 167 cod. Privacy, così come modificato dal Dlgs 101/2018 e comunque di qualsivoglia violazione in ambito privacy, e risponderà in proprio di tutte le eventuali e possibili conseguenze sia in ambito civile che penale.

Le informazioni sul trattamento dei dati personali da parte dell'Istituto Scolastico e le modalità per l'esercizio dei diritti sono disponibili nella sezione Privacy del sito istituzionale www.icdecurtis.edu.it

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