



Ministero dell'Istruzione - Ufficio Scolastico Regionale per il Lazio

## **ISTITUTO COMPRENSIVO "DON ANDREA SANTORO"**

Via Giacomo Matteotti, snc – 04015 Priverno (LT) - Tel. 0773 905266 Fax 0773 1871345 C.F. 80004680593  
e-mail Ministeriale: [ltic84200v@istruzione.it](mailto:ltic84200v@istruzione.it) [P.E.C.ltic84200v@pec.istruzione.it](mailto:P.E.C.ltic84200v@pec.istruzione.it) [www.icdonandreasantoro.edu.it](http://www.icdonandreasantoro.edu.it)

L'istituzione scolastica, sulla base di quanto previsto dal Regolamento approvato dal Consiglio di Istituto, sentito il parere del RPD,

### ADOTTA

le seguenti, misure tecniche e organizzative al fine di garantire che i dati personali trattati nelle attività relative alla Didattica digitale Integrata (d'ora in avanti DDI) vengano protetti da trattamenti non autorizzati o illeciti, dalla perdita, dalla distruzione o da danni accidentali.

- ✓ Ogni utente potrà accedere ai servizi DDI attraverso procedure di identificazione e di autenticazione informatica degli utenti;
  - l'assegnazione agli utenti di credenziali o dispositivi di autenticazione avviene a cura del personale dell'Istituto incaricato/nominato che avrà cura di assegnare password complesse o in alternativa con il contributo dei tutori dei minori
- ✓ A ciascun utente viene assegnato un profilo di autorizzazione in modo da garantire un accesso selettivo ai dati. Ove si rende necessario/conveniente l'utente viene assegnato alla classe virtuale di appartenenza;
- ✓ Password policy:
  - 11 caratteri alfanumerici con maiuscole e minuscole e caratteri speciali
  - Cambio obbligatorio ogni tre mesi
  - NON SALVARE le password di accesso;
  - Effettuare il logout (disconnessione) alla fine di ogni sessione di lavoro;
  - Accesso esclusivo alla visualizzazione delle informazioni personali una volta loggati e si svolgono operazioni su dati presenti nelle piattaforme. Assicurarsi che nessuno anche tra familiari ed amici possa visualizzare le informazioni video. In caso di momentaneo allontanamento dalla postazione, effettuare il logout dalle piattaforme e spegnere la postazione di lavoro e/o utilizzare altri strumenti tecnici (screen saver con password) per impedire la visualizzazione di documenti con dati personali salvati sul dispositivo anche accidentale.
- ✓ Impostazione della piattaforma DDI al cambio obbligatorio e conservazione delle password degli utenti, mediante l'utilizzo di funzioni di hashing allo stato dell'arte (es. PBKDF2, bcrypt, ecc.) e di salto di lunghezza adeguata;
- ✓ utilizzo di canali di trasmissione crittografati con certificato SSL (<https://>);
- ✓ Impostazione di misure atte a garantire la disponibilità dei dati attraverso il profilo di amministrazione e/o attraverso piano hosting adeguato (backup giornaliero, settimanale e mensile);
- ✓ Al fine di prevenire la vulnerabilità dei sistemi ogni utente dovrà accedere alle piattaforme DDI attraverso dispositivi che le seguenti caratteristiche:
  - Sistema operativo Windows 10 o 8 con installate le patch di sicurezza (aggiornato). Per i dispositivi con sistemi operativi diversi (Apple, Linux, IOS,

- Android) il sistema operativo deve essere aggiornato alla versione più recente o al limite la precedente
- Sistemi antivirus e anti malware settati in modalità aggiornamento automatico
  - Utilizzo di applicazioni (es: browser web, editor di testo) aggiornate alla versione più recente
  - Utilizzo di connessioni sicure su reti note in fibra o ADSL
- ✓ Sul server sul quale è installato la piattaforma DDI siano presenti sistemi antivirus e anti malware settati in modalità aggiornamento adeguato;
  - ✓ Le piattaforme DDI registrazione degli accessi e delle operazioni compiute in appositi file di log, ai fini della verifica della correttezza e legittimità del trattamento dei dati;
  - ✓ I soggetti autorizzati (docenti, tecnici) ricevono formale incarico e istruzioni operative;
  - ✓ L'animatore digitale verifica che le impostazioni di sicurezza definite in questo documento per la parte di competenza vengano rispettate e opera di concerto con l'amministratore di sistema e i fornitori delle piattaforme tecnologie.
  - ✓ Formazione e sensibilizzazione degli utenti sia per ciò che concerne gli aspetti tecnici per l'accesso e uso delle piattaforme DDI, che per ciò che attiene ai rischi di perdita e divulgazione dei dati. Deve essere ben noto a tutti gli utilizzatori delle responsabilità civili e penali in caso di divulgazione, diffusione non autorizzata di informazioni personali
  - ✓ Durante le videolezioni in modalità sincrona il docente/relatore attraverso disclaimer o indicazioni richiama le responsabilità di cui al punto precedente, si accerta che i partecipanti abbiano i requisiti per accedere escludendo eventuali intrusi.
  - ✓ Il puntamento delle telecamere utilizzate nelle videolezioni deve essere tale da assicurare la visione del solo volto del partecipante e non aree private.
  - ✓ Il riuso delle videolezioni effettuato in modalità sincrona opportunamente registrate è ammissibile previa verifica di:
    - Ammissibilità secondo le norme che disciplinano il lavoro
    - Utilizzo da parte da parte di utilizzatori della stessa classe (es studenti assenti)
  - ✓ I fornitori di tecnologie in cloud verranno nominati responsabili esterni.
  - ✓ Nel caso i server in cloud risiedano al di fuori dell'Unione Europea vanno verificati i presupposti giuridici per assicurare un adeguato livello di protezione dei dati
  - ✓ Non sono ammessi sistemi di tracciamento delle visite (analytics), notifiche push, font resi disponibili da terze parti, sistemi di advertising e in-appurchasing
  - ✓ Non è ammesso l'accesso alle piattaforme tramite sistemi di Social Login
  - ✓ Per i sistemi di messaggistica su Smartphone (WhatsApp) si sconsiglia vivamente la gestione congiunta di un gruppo genitori-docenti e comunque i messaggi dovrebbero essere inviati sempre in modalità broadcast.
  - ✓ Rispetto delle procedure definite nel Regolamento per l'utilizzo delle Piattaforme DDI
  - ✓ Divulgazione e sensibilizzazione a tutti gli utilizzatori in particolare studenti e allievi del Regolamento e delle principali regole di sicurezza da tenere.