# Allegato per Comodato pc/notebook Policy protezione dati dispositivi di proprietà dell'Itis Volta

**Premessa**

L'Itis "A. Volta", (di seguito Istituto) può consentire ad alcuni dei suoi studenti, detentori di dispositivi di proprietà dell'Istituto, di connettersi ad alcuni indirizzi di posta elettronica riconducibili all'Istituto e altri sistemi informatici[1] o di svolgere attività scolastiche di studio da un luogo esterno alla sede di spalto Marengo, 42 - Alessandria. L'Istituto si riserva il diritto di interrompere questo servizio se gli studenti non si attengano alle politiche e procedure descritte di seguito.

**Finalità**

Questa procedura è volta a proteggere la sicurezza e l'integrità dell'infrastruttura dati e tecnologica dell'Istituto. Eccezioni limitate alla politica possono verificarsi a causa di variazioni nei dispositivi e piattaforme.

Gli studenti devono accettare i termini e le condizioni stabilite in questa politica per essere in grado di collegare in sicurezza i dispositivi alla rete.

Lo svolgimento dell'attività di studio a distanza è una "modalità di lavoro innovativa e basata su un forte elemento di flessibilità, in modo particolare di orari e di sede; allo studente viene lasciata ampia libertà di auto-organizzarsi a patto che porti a termine gli obiettivi stabiliti nelle scadenze previste, rispettando in ogni caso la data di consegna dei compiti assegnati e gli orari di lezione e interrogazione online stabilite dai docenti".

Tenuto conto dell'impossibilità di controllare in modo continuo lo svolgimento dell'attività di studio a distanza l'Istituto adotta le seguenti misure:

a) consegna allo studente che svolge la prestazione simile al regime di "smartworking – lavoro agile" un'informativa nella quale "sono individuati in via indicativa i rischi generali e i rischi specifici connessi alle modalità di svolgimento della prestazione e le misure di prevenzione da adottare;

b) fornisce allo studente strumenti informatici e/o telematici conformi agli attuali standard tecnici e normativi, costantemente aggiornati;

c) presta cura adeguata nel consigliare i comportamenti idonei a garantire lo svolgimento in sicurezza della prestazione studentesca.

[1] Posta elettronica - È fatto divieto di utilizzare la posta elettronica per motivi diversi da quelli strettamente legati all'attività di studio. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:
- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività di studio;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing list;
- la partecipazione a catene telematiche (o c.d. "di Sant'Antonio").

Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al coordinatore della classe. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.
Le medesime precauzioni dovranno essere adottate nell'uso di social media autorizzati, quali a titolo esemplificativo WhatsApp.
In particolare il Registro Elettronico, la Segreteria Digitale (SD) e Moodle dovranno essere utilizzati esclusivamente per finalità scolastiche riconosciute dall'Istituto.

E, a sua volta, lo studente "coopera con diligenza all'attuazione delle misure di prevenzione predisposte dall'Istituto".

**Uso corretto**

L'uso corretto dei dispositivi affidati allo studente è finalizzata a consentire e migliorare l'attività scolastica. Gli studenti possono utilizzare il dispositivo mobile dell'Istituto per svolgere attività descritte nelle Finalità del presente documento. L'uso extra scolastico è da ritenersi corretto e accettabile solo se consistente in una comunicazione personale ragionevole e limitata per motivi personali.

**Restrizioni**

Gli studenti si impegnano a non accedere ai siti web non correlati all'attività di studio e durante il collegamento alla rete dell'Istituto[2].

I dispositivi affidati agli studenti non possono essere utilizzati in alcun modo per:

1. conservare o trasmettere materiali illeciti;

2. memorizzare o trasmettere informazioni proprietarie al di fuori delle finalità;

3. molestare gli altri;

4. impegnarsi in attività esterne non scolastiche;

5. Non è consentito l'uso di applicazioni o software non scaricati da fornitori o portali riconosciuti come Microsoft, iTunes, Google Play ecc.;

**Sicurezza**

Al fine di impedire l'accesso non autorizzato, i dispositivi devono essere protetti da password utilizzando le caratteristiche del dispositivo ed è necessaria una password forte per accedere alla rete dell'Istituto.

La politica di protezione dell'Istituto è:

[2] In particolare occorre evitare.
- l'upload o il download di software anche gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività di studio (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il coordinatore di classe)
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività di studio;
- la partecipazione a Forum non professionali, l'iscrizione con account scolastico e la partecipazione personale a social network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati;
- l'accesso, tramite internet, a caselle webmail di posta elettronica personale escluse le connessioni legate alla didattica.

• Le password devono contenere almeno otto caratteri e una combinazione di lettere maiuscole e minuscole, numeri e simboli.

• L'accesso degli studenti ai dati dell'Istituto è determinato di volta in volta dalla Dirigenza.

• Il dispositivo deve bloccarsi con una password (es. password screensaver) o un PIN o un riconoscimento biometrico se inattivo. Il tempo di blocco deve essere impostato al più basso tempo disponibile.

• Conservare le apparecchiature in uno spazio sicuro, asciutto e pulito quando non sono in uso.

• L'accesso alla rete di Istituto utilizzando dispositivi soggetti a manipolazioni come il Rooted (Android) o jailbroken (iOS) sono severamente vietate.

• L'Istituto si riserva il diritto di installare e utilizzare la tecnologia di cancellazione remota sul dispositivo dell'utente. Il dispositivo può essere cancellato da remoto se

1) il dispositivo è perso,

2) avviene la cessazione del rapporto di comodato d'uso tra lo studente e l'Istituto,

3) l'Istituto viene a conoscenza di una violazione dei dati o delle politiche, di un virus o di una minaccia simile per la sicurezza dei dati e delle infrastrutture tecnologiche dell'Istituto.

Lo smarrimento o il furto dei dispositivi devono essere segnalati all'Istituto entro 24 ore. Se necessario lo studente è tenuto a informare immediatamente anche il proprio gestore mobile in tali casi.

Lo studente è tenuto ad utilizzare i dispositivi in modo etico in ogni momento e ad attenersi alla politica di utilizzo accettabile dell'Istituto come sopra descritto.

Lo studente è personalmente responsabile per tutti i costi associati al dispositivo.

**Dispositivi e Supporto**

Gli studenti non devono contattare direttamente il fabbricante del dispositivo o il loro distributore per tutte le questioni relative al sistema operativo o all'hardware. Problemi tecnici possono essere supportati dall'Istituto.

I dispositivi devono essere mantenuti con la corretta configurazione di applicazioni standard, come browser e strumenti di sicurezza, prima di poter accedere alla rete.

**Rischi e Responsabilità**

Mentre l'Istituto prenderà ogni precauzione per evitare che i propri dati personali di proprietà dello studente vengano persi nel caso in cui si debba manipolare o resettare da remoto un dispositivo, è responsabilità dello studente prendere ulteriori

precauzioni per la responsabilità per i propri dati personali di proprietà, come il backup di e-mail personali, contatti, foto, documenti ecc.

L'Istituto si riserva il diritto di disconnettere i dispositivi dal proprio sistema o disabilitare i servizi senza preavviso.

Lo studente si assume piena responsabilità per i rischi correlati alla perdita parziale o completa dei propri dati personali a causa di un crash del sistema operativo, errori, bug, virus, malware e/o altri guasti software o hardware, o errori di programmazione che rendono il dispositivo inutilizzabile.

L'Istituto si riserva il diritto di intraprendere azioni adeguate nei confronti degli studenti, comprese: azioni legali, risoluzione del contratto di comodato, applicazione di procedure disciplinari per inosservanza della presente Policy di protezione dati dispositivi.

Il Dirigente scolastico
Dott.ssa Maria Elena DEALESSI

……..

Alessandria, 06 aprile 2020

Lo studente con la sottoscrizione accetta questa Policy di protezione dati dispositivi

Firma: .....

Il genitore dello studente minore con la sottoscrizione accetta questa Policy di protezione dati dispositivi

Firma: .....