Regolamento informatico d'Istituto – P.U.A.

Preambolo

Scopo del presente Regolamento è informare e formare l'utenza scolastica in merito all'uso corretto e responsabile dei device e degli strumenti informatici in dotazione alla Scuola, nel rispetto della normativa vigente. Tale documento mira altresì a normare l'utilizzo della rete all'interno dell'Istituto, a fornire indicazioni chiare ed esaustive sull'uso della Google Suite Workspace e del Registro elettronico da parte del personale, degli studenti e dei genitori e a definire i lineamenti fondamentali della **P.U.A.** (*Politica d'Uso Accettabile della Rete*). In appendice esso riporta anche il **BYOD** (*Bring Your Own Devices* – "Porta il tuo dispositivo") d'Istituto.

La fissazione delle norme che seguono è cogente per i differenti ordini e gradi scolastici del Collegio Arcivescovile; la sua esplicitazione si manifesta come una necessità, visto il massiccio impatto che internet ha sull'attuale società e, a *fortiori*, sul *sistema scuola*.

Oltre ad essere un'agenzia formativa, la scuola è una comunità di ricerca e di esperienza sociale, volta alla crescita della persona in tutte le sue dimensioni. Essa fornisce servizi educativi specifici e pianificati, avvalendosi di tecniche e metodi che vengono elaborati da un'apposita disciplina, la didattica. La recente diffusione delle tecnologie informatiche ha un'importante ricaduta su tale ambito: il curricolo scolastico prevede, per ogni ordine e grado, che gli alunni imparino ad utilizzare le Tic (*Tecnologie dell'informazione e della comunicazione*). Per questo i Collegi docenti d'Istituto ritengono importante promuovere l'uso delle Tic come supporto dei processi di insegnamento/apprendimento, nell'ottica di una didattica inclusiva, capace di promuovere al tempo stesso l'eccellenza in ambito didattico attraverso la condivisione delle risorse, ai fini del successo formativo, cognitivo e psico-sociale degli alunni.

Nel definire il presente documento i Collegi docenti d'Istituto sottoscrivono i seguenti presupposti estrapolati dalle Linee guida del MIUR relative al *Piano Nazionale Scuola Digitale* (PNSD), da osservare e tener presenti allo scopo di promuovere la crescita civica e sociale dei propri alunni:

- lo sviluppo del digitale nella didattica va accolto quale fattore di innovazione e chiede di essere gestito adeguatamente dal sistema-scuola per migliorare l'apprendimento degli alunni e, in generale, il benessere sociale e lavorativo della comunità scolastica;

- i dispositivi di comunicazione online e internet devono essere un mezzo, non un fine, per sviluppare negli alunni abilità tecniche nuove e valide e sostenere in loro lo sviluppo di una capacità critica e creativa;

- occorre sostenere nelle giovani generazioni un approccio consapevole e autonomo al digitale, in previsione di un *long life learning* sull'uso critico delle fonti di informazione;

- le tecnologie digitali devono essere funzionali a rafforzare la coesione della comunità scolastica nel suo complesso, l'esercizio della didattica e l'alleanza educativa con le famiglie;

- educare alla cittadinanza digitale è un dovere per la scuola. Formare i futuri cittadini della società della conoscenza significa educare alla partecipazione responsabile, all'uso critico delle tecnologie, alla consapevolezza e alla costruzione delle proprie competenze in un mondo sempre più connesso.

Con riferimento specifico al BYOD, occorre dire che il ricorso a politiche attive per l'utilizzo di dispositivi tecnologici *personali* in ambito educativo/scolastico viene espressamente previsto, attraverso una specifica azione, dal Piano Nazionale Scuola Digitale e, in particolare, dal documento di indirizzo del *Ministero dell'Istruzione dell'Università e della Ricerca* "per il lancio di una strategia complessiva di innovazione della scuola italiana e per un nuovo posizionamento del suo sistema educativo nell'era digitale".

L'azione *#6* del PNSD "*Politiche attive per il BYOD*" vuole garantire a tutti gli studenti una formazione digitale che inizi con il saper usare i propri dispositivi. Poiché la tecnologia fornisce agli studenti opportunità innovative ed inedite per incrementare la loro cultura, il nostro Istituto intende favorire tale processo garantendone l'effettiva sicurezza.

Art. 1 - Utilizzo di PC, tablet, LIM, notebook, stampanti e altri strumenti informatici della scuola

Le sedi scolastiche del Collegio dispongono di laboratori informatici, LIM, stampanti e vari device fissi o portatili ad esclusivo uso didattico. Alunni, docenti ed educatori possono utilizzarli a condizione di avere cura dei componenti hardware e software di tali strumenti. Le apparecchiature presenti nella Scuola sono un patrimonio comune: vanno quindi utilizzate con il massimo rispetto e minimizzando gli sprechi di risorse (energia, carta, toner, etc.).

Gli insegnanti sono responsabili degli strumenti che stanno utilizzando e hanno il compito di sovrintendere sul loro utilizzo e di responsabilizzare anche gli alunni, per renderli consapevoli dell'importanza della salvaguardia di un bene comune. In caso di danno che non risulti evidentemente accidentale, il responsabile sarà tenuto a risponderne pecuniariamente.

Salvo esplicita autorizzazione del referente informatico del Collegio non è consentito:

- modificare il sistema operativo o le sue impostazioni generali;

- installare e disinstallare i programmi o modificarne le impostazioni (ivi incluse le estensioni dei browser);

- scaricare o caricare software non legati alle finalità didattiche;

- modificare le impostazioni per l'accesso alla rete o installare modem o altri dispositivi per l'accesso indipendente ad internet;

- utilizzare le stampanti, CD, DVD o altro a fini personali;

- usare gli strumenti informatici della scuola per scopi diversi da quelli didattici e di studio;

- copiare, caricare o scaricare musica, film, programmi e qualsiasi altro materiale non legato alla didattica o vincolato da copyright o comunque in conflitto con le norme dei codici civile e penale riguardanti il diritto d'autore, la privacy, la divulgazione di materiale offensivo, pedo-pornografico etc.

Agli utenti è fatto espresso divieto di influenzare negativamente la regolare operatività degli strumenti e della rete, interferire con la connettività altrui o con il funzionamento del sistema e quindi di: utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti; leggere, copiare o cancellare files e software altrui; utilizzare software rivolti alla violazione della sicurezza del sistema; sostituirsi a qualcuno nell'uso dei sistemi; cercare di catturare password altrui o forzare password o comunicazioni elettroniche; limitare o negare l'accesso al sistema a utenti legittimi; effettuare trasferimenti non autorizzati di informazioni (software, dati personali, ecc.); distruggere o alterare dati altrui.

Qualora un utente dovesse riscontrare malfunzionamenti, guasti o situazioni di rischio per la sicurezza o l'integrità del sistema deve darne immediata comunicazione al Preside o all'amministratore di sistema. Salvo preventiva espressa autorizzazione non è consentito eseguire operazioni di manutenzione ordinaria o straordinaria autonomamente.

Art. 2 - Accesso alla rete Wi-fi d'Istituto

In ogni plesso del Collegio Arcivescovile è possibile connettersi ad internet mediante cavo di rete o via Wi-fi. Tutti i computer e tablet della scuola sono già impostati per accedere direttamente alla rete tramite credenziali di accesso personali e riservate; il personale scolastico può accedere con device privati richiedendo le credenziali di accesso e impegnandosi a non perderle né divulgarle. Qualsiasi device assegnato al personale della scuola ed abilitato alla navigazione in internet costituisce uno strumento utilizzabile esclusivamente per lo svolgimento dell'attività lavorativa. È quindi assolutamente proibita la navigazione in internet per motivi diversi da quelli strettamente legati alla stessa.

Art. 3 - Utilizzo della Google Suite da parte del personale, degli studenti, dei genitori

Il nostro Istituto ha al suo attivo il dominio *arcivescoviletrento.it* associato alla piattaforma di Google "G-Suite for Education". Tutto il personale ottiene, al momento dell'assunzione da parte del Collegio, un account istituzionale (secondo la tipologia "*nomecognome@arcivescoviletrento.it*") con cui accedere e lavorare in ambiente Google a titolo gratuito e in modo protetto, utilizzando i servizi di posta elettronica, archivio Drive, creazione di documenti e numerose altre applicazioni. La stessa opportunità è offerta agli alunni del Collegio.

Per ulteriori informazioni sulla configurazione della piattaforma, sui termini del servizio e sulle informative riferite al trattamento dati personali si fa rinvio ai seguenti link:

- https://support.google.com/a/answer/60762?hl=it;
- https://www.google.com/policies/terms/;
- https://www.google.com/policies/privacy/.

L'attivazione di tale servizio per gli alunni comporta necessariamente la consapevole accettazione di quanto segue:

- l'utilizzo dei predetti strumenti prevede una procedura di autenticazione personale. Le credenziali (nome utente e password) sono segrete e non possono essere cedute a terzi. Ogni assegnatario è responsabile di tutti i comportamenti eseguiti attraverso il proprio account;
- la posta elettronica e tutte le applicazioni abilitate devono essere utilizzate esclusivamente per svolgere attività didattiche secondo le indicazioni della Dirigenza, dei Collegi dei docenti o dei docenti responsabili delle lezioni;
- tutti gli strumenti e l'indirizzo di posta elettronica dovranno essere utilizzati solo per scopi didattici e non per attività esterne;
- il rapporto per l'uso dei predetti strumenti ha durata annuale e viene rinnovato automaticamente all'atto dell'iscrizione. L'account sarà cancellato finito il percorso di studio presso l'Istituto;
- per nessuna ragione è consentito scaricare o caricare nulla sui device scolastici a fini personali (file musicali, foto, software, video, etc.), tranne nel caso di specifiche attività didattiche preventivamente programmate e regolamentate dai docenti;

- l'Istituto prenderà tutte le precauzioni per garantire che gli studenti non abbiano accesso a materiale non adeguato, pur sapendo che è oggettivamente impossibile azzerare tale rischio; pertanto, si accetta come condizione necessaria al mantenimento della sicurezza interna all'Istituto che in qualsiasi momento i docenti amministratori possano accedere all'account degli alunni per verificare ed eventualmente sospendere l'account di coloro che facciano un uso improprio di questo servizio.

Tutto il personale scolastico deve tenere presente che:

- le credenziali di accesso (nome utente e password) sono strettamente personali, non possono essere cedute a terzi ed ogni attività non regolare sarà imputata al titolare delle credenziali;

- l'utilizzo delle caselle di posta elettronica e del sistema informatico della scuola non è consentito per attività personali non attinenti la didattica o la propria attività istituzionale;

- è possibile iscriversi a siti, blog, forum o altro utilizzando l'account di *arcivescoviletrento.it* solo ed esclusivamente per finalità didattiche o istituzionali;

- la riservatezza dei dati condivisi in Drive è responsabilità in primis del proprietario del file e, a seguire, di chi ha accesso al file in condivisione;

- è vietato diffondere dati personali, immagini e registrazioni delle lezioni in remoto nonché utilizzare gli strumenti digitali per produrre, condividere e diffondere contenuti offensivi della dignità di terzi.

A tutela della privacy di tutti i nostri utenti, si fa presente che Google Suite for Education possiede un sistema di controllo che permette all'amministratore di sistema di verificare quotidianamente i cosiddetti "log di accesso" alla piattaforma. È possibile ad esempio monitorare, in tempo reale, le sessioni di videoconferenza aperte, l'orario di inizio/termine della singola sessione, i partecipanti che hanno avuto accesso e il loro orario di ingresso e uscita. La piattaforma è quindi in grado di segnalare tutti gli eventuali abusi, occorsi prima, durante e dopo ogni sessione di lavoro.

L'amministratore del servizio può gestire gli accessi alle applicazioni attribuendo agli utenti diversi livelli di autonomia a seconda dei ruoli e delle funzioni. Se si dovesse rendere necessario per fini di sicurezza interna, tutti gli account potranno essere sottoposti a verifica e/o sospesi dall'amministratore del servizio.

Eventuali comportamenti difformi alle presenti condizioni possono portare all'attribuzione di note disciplinari e all'immediata convocazione a colloquio dei genitori, e, nei casi più gravi, all'irrogazione di sanzioni disciplinari con conseguenze sulla valutazione intermedia e finale del comportamento.

Art. 4 - Utilizzo del Registro elettronico

Il Registro elettronico, il cui utilizzo è previsto per Legge dal D.L. 6 luglio 2012 n. 95, convertito dalla legge 7 agosto 2012 n. 135, è un applicativo finalizzato alla dematerializzazione, allo snellimento delle procedure e a garantire e promuovere l'accesso all'informazione da parte di studenti e famiglie. Il Collegio Arcivescovile ha adottato l'applicativo Mastercom per gestire il Registro di classe, il Registro dei docenti, le pagelle, gli scrutini, le udienze e alcune comunicazioni con le famiglie. Tutte le operazioni relative all'uso del Registro elettronico sono improntate alla tutela della privacy ed ogni tipologia di utente ha accesso solo ad informazioni strettamente pertinenti al proprio ruolo. Tutti i docenti dell'Istituto e i genitori degli alunni possono accedere al Registro elettronico dal portale Mastercom. La segreteria consegna ad ogni utente username e password per accedere ad esso: tali credenziali sono strettamente personali e sarà cura di ogni utente garantirne la riservatezza. Ogni attività non regolare sarà imputata al titolare delle credenziali.

Art. 5 - Responsabilità individuali in merito al rispetto della privacy, tutele del copyright e sicurezza informatica

Docenti e alunni devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Poiché esiste la concreta possibilità che durante il lavoro online portato avanti in ambito scolastico si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale, il Collegio promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti. Dato che non è possibile garantire una navigazione totalmente priva di rischi, la Scuola e i docenti non possono assumersi le responsabilità conseguenti all'accesso accidentale e/o improprio a siti illeciti, o al reperimento ed uso di materiali inappropriati. Qualora questo dovesse verificarsi, la scuola prenderà tutti i provvedimenti necessari per sanzionare chiunque si sia reso responsabile di comportamenti scorretti e ridurre la possibilità che questi si ripetano in futuro, inclusa la segnalazione alle forze dell'ordine o agli enti preposti nei casi di maggiore gravità.

Ogni docente, prima di far accedere i propri studenti ad una qualsiasi risorsa informatica, si impegna a:

- illustrare ai propri alunni le regole di utilizzo contenute nel presente documento e controllare che il loro accesso alla rete fornita a scuola avvenga sempre e solamente sotto la propria supervisione;

- dare chiare indicazioni sul corretto utilizzo della rete (internet, piattaforme studenti, ...) e sulla prevenzione dei rischi ad essa connessi;

- assumersi la responsabilità della tracciabilità dell'utilizzo e del mantenimento in buono stato della strumentazione tecnologica utilizzata da lui stesso e dagli alunni, segnalando prontamente eventuali malfunzionamenti o danneggiamenti al referente informatico del Collegio;

- non divulgare le credenziali di accesso agli account e alla rete Wi-fi;

- non lasciare incustodite le postazioni con cui ha fatto accesso agli account istituzionali (Registro elettronico, sito scolastico, Gmail, …), se non dopo essersi disconnesso;

- non salvare sulla memoria locale dei PC o di altri device della scuola file contenenti dati personali e/o sensibili e tutelare la propria privacy e quella altrui non divulgando notizie private contenute nelle documentazioni elettroniche a cui ha accesso.

Nel contesto dell'attività di didattica a distanza (DAD) si raccomanda l'attenzione sui seguenti punti:

- se si utilizzano device privati (es PC, notebook, ecc.) verificare che tali strumenti siano dotati delle basilari misure di sicurezza (tra cui un sistema operativo aggiornato, un antivirus/antimalware, un firewall, una procedura di accesso (log-in) mediante password (che deve essere personale e segreta), un piano di back up, ecc.). In caso negativo, adottare tali semplici misure di protezione;

- nella scelta dei software più utili per la realizzazione della didattica a distanza è necessario ricorrere unicamente a strumenti che abbiano fin dalla progettazione e per impostazioni predefinite misure a protezione dei dati personali degli alunni;

- nel caso in cui si utilizzino piattaforme web, si dovranno attivare i soli servizi strettamente necessari alla formazione, configurandoli in modo da minimizzare i dati personali da trattare (evitando, ad esempio, geolocalizzazione e social login);

- evitare di fare ricorso all'utilizzo di chiavette USB per la gestione di dati personali degli alunni se tali strumenti sono privi di un sistema protezione e di cifratura;

- utilizzare sempre connessioni sicure alla rete internet e, in caso di collegamento mediante reti Wi-fi, fare in modo che l'accesso a queste sia protetto da password;

- elevare il grado di complessità delle password che si utilizzano, prevedendo il loro frequente cambiamento;

- non lasciare incustoditi i dispositivi elettronici ed evitare che terzi possano accedere alle informazioni lavorative in essi conservate. Il salvataggio del materiale lavorativo contenente dati personali è permesso se strettamente necessario e comunque in cartelle protette, meglio se cifrate;

- se si utilizzano sistemi di posta elettronica per l'inoltro di messaggi a più destinatari è opportuno fare in modo di non mettere in condivisione e/o lasciare in chiaro i loro indirizzi;

- se si utilizzano spazi di condivisione è necessario valutare a monte quali informazioni possano essere condivise con tutti coloro che vi accedono e quali invece devono rimanere protette e riservate attraverso uno scambio esclusivo e diretto con l'interessato;

- informare sempre gli interessati con un linguaggio facilmente comprensibile, in merito alle modalità di erogazione della didattica a distanza specificando quali sono i dati trattati, le modalità di trattamento degli stessi, i tempi di conservazione e le operazioni di trattamento che verranno eseguite;

- l'utilizzo di servizi in cloud potrebbe essere potenzialmente pericoloso e pertanto deve avvenire tramite gli strumenti espressamente autorizzati dalla nostra scuola. In caso fosse necessaria l'attivazione di possibili nuovi sussidi tecnologici si invita ciascun insegnante a confrontarsi preventivamente con il Preside;

- prevedere e incentivare la supervisione dei genitori sul corretto utilizzo di tutti gli strumenti messi a disposizione degli alunni per favorire la didattica a distanza e condividere con loro la logica della minimizzazione nel trattamento dei loro dati personali;

- se ci si dovesse accorgere di aver subito un incidente di sicurezza ("data breach") comunicare immediatamente quanto occorso al Preside;

- evitare l'uso di social network o di altre applicazioni facilmente hackerabili per il trattamento di dati personali connesso allo svolgimento di attività lavorativa. Anche in tal caso, laddove necessario, condividere con il Preside l'attivazione di nuove soluzioni;

- fare in modo che la condivisione di informazioni e lo scambio di materiale mediante sistemi di messaggistica istantanea si svolga prestando attenzione che i contenuti siano rivolti agli effettivi destinatari e non a terzi.

Gli alunni, da parte loro, sono tenuti a:

- comunicare immediatamente al docente della lezione eventuali malfunzionamenti della strumentazione o accessi accidentali a informazioni, immagini, applicazioni o altro materiale non appropriato;

- non eseguire tentativi di modifica della configurazione di sistema dei computer o di qualsiasi altro device che si stia utilizzando;

- non condividere le proprie credenziali di autenticazione, proteggendo e mantenendo le stesse riservate;

- accedere alla rete solo in presenza del docente e dopo esplicita autorizzazione da parte sua;
- non utilizzare la strumentazione della scuola a scopi personali, ludici, ricreativi;
- non utilizzare device personali senza autorizzazione da parte del docente;
- chiudere correttamente la propria sessione di lavoro e uscire dal proprio account tutte le volte che si lascia una postazione.

Tutti gli utenti informatici, siano docenti o alunni, si impegnano, altresì, al rispetto delle norme di buon utilizzo del servizio ed in particolare a quanto segue:

- non trasmettere, distribuire, diffondere, condividere o mantenere qualsiasi tipo di materiale in violazione delle norme vigenti (questo include, senza limitazioni e a mero titolo esemplificativo, materiale protetto da copyright, marchi registrati, segreti industriali o altre proprietà intellettuali, materiale pornografico, diffamatorio o che costituisce trattamento illecito di dati personali o viola le leggi sul controllo delle esportazioni);
- non procedere all'invio massivo di mail non richieste (spam);
- non fare pubblicità a nessun tipo di prodotto o servizio;
- non scaricare né trasmettere nessun tipo di software, programma, prodotto o servizio che violi il presente Regolamento o le norme vigenti;
- utilizzare esclusivamente le risorse per cui hanno ottenuto l'autorizzazione;
- evitare qualsiasi attività che possa produrre danni alle risorse informatiche del Collegio Arcivescovile o di terzi, comprometterne la sicurezza o la riservatezza delle risorse;
- segnalare ogni accertata violazione delle norme del presente Regolamento all'amministratore del servizio.

Art. 6 - Gestione del sito web della scuola

Il webmaster e i collaboratori interni designati dalla Dirigenza gestiscono le pagine del sito ed è loro responsabilità garantire che il contenuto del sito sia accurato e appropriato. L'Istituto detiene i diritti d'autore dei documenti e delle foto che si trovano sul sito. Le informazioni pubblicate sul sito d'Istituto relative alle persone (alunni, docenti, personale amministrativo, ecc.) devono includere solo l'indirizzo di posta elettronica e il telefono d'Istituto, non informazioni relative al loro profilo privato.

Art. 7 - Trattamento dei dati e limitazioni di responsabilità

Sono interdetti al datore di lavoro controlli del personale dipendente effettuati in maniera diretta, prolungata, costante o indiscriminata (art. 4, Statuto dei lavoratori, l. 300/1970). Ciò premesso, oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, etc.), comunque estranei a qualsiasi finalità di controllo diretto dell'attività lavorativa, è facoltà del titolare tramite gli addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

Il titolare può avvalersi di sistemi di controllo relativi al corretto utilizzo degli strumenti informatici messi a disposizione dei propri collaboratori e dipendenti che consentano indirettamente un controllo a distanza sull'effettivo adempimento della prestazione lavorativa: tali controlli saranno effettuati qualora le misure minime preventivamente esposte non siano state sufficienti per evitare comportamenti anomali. I controlli saranno svolti con gradualità, secondo i principi di pertinenza e non eccedenza. In seguito si espongono le modalità di esercizio di tali controlli: in prima battuta si effettuerà un controllo preliminare su dati anonimi ed aggregati; si procederà pertanto con verifiche di ufficio o gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole prestabilite.

Il controllo anonimo può dare atto ad un avviso di rilevazione di un utilizzo inadeguato degli strumenti aziendali; contestualmente si diramerà una nota di richiamo invitando tutti i dipendenti e collaboratori ad attenersi ai compiti e alle mansioni impartite tenuto conto del dovere di conformarsi alle presenti regole. Se si dovesse ripetere l'anomalia sarà facoltà del Collegio procedere con controlli mirati, anche su base individuale, e successivamente, in caso di infrazioni, adottare sanzioni disciplinari. L'adozione delle sanzioni disciplinari avverrà a norma dell'art. 2106 c.c. del codice civile, dell'art. 7 dello statuto dei lavoratori (legge 300/1970), del contratto di riferimento e del relativo codice disciplinare vigente. I dati contenuti nei file di log, relativi agli accessi ad internet e al traffico telematico, possono essere conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza. I file di log potranno essere utilizzati in tali casi: a) produzione di report statistici che presentino i dati relativi alla navigazione in forma aggregata e anonima; b) per l'analisi dei problemi riscontrati nel sistema e soluzione dei medesimi, estraendo i dati in modo aggregato e in forma anonima.

Tutto il personale scolastico, docente e non docente, è coinvolto nel monitoraggio dell'utilizzo delle risorse informatiche da parte degli alunni, nello sviluppo delle linee guida e nell'applicazione delle istruzioni sull'uso sicuro e responsabile di internet. Il preside e i singoli docenti che riscontrino negli alunni comportamenti non in linea con il presente Regolamento hanno il diritto di revocare, in modo temporaneo o permanente, l'accessibilità ai laboratori informatici e/o l'utilizzo di strumenti tecnologici (tablet, notebook, account di Google etc.) da parte degli alunni. Il Collegio Arcivescovile

non assume alcuna responsabilità in merito a danni, perdite e costi subiti o causati dagli utenti a seguito della violazione delle norme contenute in tale documento. Oltre al rispetto del presente regolamento è fatto obbligo di attenersi scrupolosamente alle disposizioni in materia di trattamento dati personali e alle relative misure di sicurezza (come indicate nella lettera di designazione di incaricato del trattamento e nel materiale formativo messo a disposizione di ciascun collaboratore e dipendente) osservando con attenzione le prescrizioni del Reg. UE 16/679. Ciascun incaricato è tenuto a mantenere un costante flusso informativo con il responsabile per la protezione dei dati personali (DPO) designato dalla scuola, segnalando a quest'ultimo ogni eventuale criticità o episodio di violazione.

Regolamento BYOD (Bring Your Own Devices) per l'utilizzo dei dispositivi digitali personali a scuola

Il Piano Nazionale Scuola Digitale, previsto dalla Legge 107/2015 di riforma del sistema dell'Istruzione all'art. 1 comma 56, adottato dal MIUR, con D.M. n. 851 del 27.10.2015, riporta, tra quelle previste, l'azione #6 "*Politiche attive per il BYOD - Bring your own device*". Nel piano generale di innovazione didattica, che richiede l'adeguamento delle metodologie didattiche e delle strategie adottate con gli alunni in classe, ruolo importante hanno le tecnologie per la didattica, da usare in maniera consapevole e ragionata (si ricorda peraltro che la competenza digitale è una delle competenze chiave per l'apprendimento permanente, identificate dall'Unione Europea).

In quest'ottica, si rende necessario garantire a tutti gli studenti un'adeguata formazione anche nell'utilizzo del digitale, che preveda anche la formazione ad un uso consapevole dei propri dispositivi. L'adozione di politiche BYOD consente al Collegio Arcivescovile di avviare una riflessione, insieme ai suoi docenti e ai genitori dei propri alunni, sulla necessità di educare bambini e ragazzi anche all'utilizzo dei propri device come occasione per fare didattica, negli spazi e nei tempi organizzati dai docenti, laddove tale pratica risulti funzionale a rendere ogni aula laboratorio, nel caso in cui non risulti di immediata disponibilità ed efficacia l'utilizzo degli spazi della scuola attrezzati come laboratorio.

L'uso di smartphone, tablet e altri dispositivi mobili, o delle funzioni equivalenti presenti sui telefoni cellulari è pertanto consentito, ma unicamente su indicazione del docente, con esclusiva finalità didattica, in momenti ben definiti e con modalità prescritte dall'insegnante.

Al di fuori di questo contesto l'uso improprio dei dispositivi digitali mobili a scuola non è ammesso e viene sanzionato in misura della gravità in base a quanto stabilito dal Regolamento di Istituto e dal Codice di disciplina, che vanno tenuti presenti per tutto quanto non concerne la sperimentazione BYOD.

a. Norme di carattere generale

1. I device ammessi a scuola e, in particolare, nelle classi appartengono alle seguenti categorie: tablet, net-book, notebook, e-reader, smartphone, smartwatch. L'uso di altri dispositivi non espressamente nominati non è consentito all'interno della scuola e delle sue pertinenze.
2. I dispositivi suddetti possono essere introdotti a scuola dagli alunni per soli scopi didattici e possono essere utilizzati dagli studenti all'interno di momenti ben definiti, solo su esplicita e chiara autorizzazione da parte degli insegnanti.
3. Ogni studente è responsabile della custodia e del corretto utilizzo del proprio device: la scuola non sarà mai ritenuta responsabile dello smarrimento, del furto o del danneggiamento del bene che, in nessun caso, dovrà essere lasciato a scuola oltre l'orario delle lezioni.
4. Per l'allievo il dispositivo mobile deve essere uno strumento funzionale all'apprendimento, pertanto rimane sua responsabilità dotarsi di un dispositivo con adeguata capienza di memoria, carica, etc. Gli studenti non possono caricare il dispositivo a scuola.

b. Limitazioni nell'uso dei dispositivi

1. Secondo le recenti indicazioni del Garante della privacy, la registrazione delle lezioni è possibile solo per usi strettamente personali e dietro esplicita autorizzazione del docente/dei docenti interessato/i. In nessun caso riprese (o foto) potranno essere eseguite di nascosto, senza il consenso dell'insegnante. Registrazioni e riprese audio/foto/video sono consentite – sempre dietro consenso dei docenti – per uso esclusivamente personale.
2. Si richiama l'attenzione degli alunni, dei docenti e delle famiglie sulle possibili conseguenze di eventuali riprese audio/video o fotografie effettuate all'interno degli ambienti scolastici, al di fuori dei casi consentiti, e successivamente diffuse con l'intento di ridicolizzare compagni o insegnanti o addirittura allo scopo di intraprendere azioni che sono spesso definite con il termine di cyberbullismo. Tali azioni possono configurare gli estremi di veri e propri reati.

c. Uso non consentito di internet

1. Agli alunni, in nessun momento delle lezioni è consentito utilizzare internet per scopi diversi da quelli didattici. Non è altresì consentito loro di scaricare musica, video e programmi da internet o qualsiasi file, a meno che l'azione non sia stata esplicitamente richiesta dai docenti e motivata dalla progettazione didattica che si sta attuando.
2. Agli studenti, in nessun momento della loro permanenza nei locali della scuola è consentito di utilizzare i propri dispositivi per attività ludiche o ricreative, se non con l'esplicito consenso degli insegnanti in base alla progettazione didattica che si sta attuando.
3. Agli alunni non è consentito utilizzare i social network durante le ore di lezione, né pubblicare foto/video, anche personali, durante la permanenza a scuola. Il divieto non si applica

soltanto all'orario delle lezioni ma è vigente anche negli intervalli, nelle pause mensa e nei momenti non strutturati.

d. Utilizzo della rete Wi-fi d'Istituto

1. La connessione alla rete Wi-fi d'Istituto da dispositivi mobili personali non è, di norma, consentita. In considerazione di esigenze didattiche particolari o di gravi problematiche personali evidenziate dai docenti, il preside potrà autorizzare singoli alunni ad accedere, temporaneamente o per l'intero anno scolastico, alla rete Wi-fi in oggetto.

e. Diritti di proprietà e copyright

1. Gli studenti devono rispettare e proteggere la proprietà intellettuale altrui: non è ammessa la copia o il plagio di qualsiasi materiale tramite internet. Nell'ambito del rispetto delle normative vigenti sui copyright e i diritti di proprietà, qualora si intenda usare materiale reperibile in rete è sempre obbligatorio citare le fonti e le sorgenti citando gli URL di provenienza attraverso il link intero. Se previsto dalla legge o da accordo, si deve richiedere il permesso degli autori o creatori delle informazioni, o dei media originali, laddove si decide di utilizzare materiale prodotto da altri.

f. Diritto/dovere di ispezione

1. Il docente che intende far usare agli alunni i loro device è responsabile nei loro confronti anche dal punto di vista della sicurezza sul web. Sarà quindi suo compito istruire i ragazzi ad un uso "in sicurezza" del dispositivo, monitorando che le indicazioni vengano rispettate.

g. Sanzioni per il mancato rispetto del presente Regolamento

1. L'uso della tecnologia, sia essa proprietà della scuola o un dispositivo fornito dagli studenti, comporta responsabilità personali. Gli studenti sono tenuti a rispettare il presente Regolamento, unitamente al Regolamento di Istituto, e ad agire responsabilmente.
2. Il mancato rispetto di questi termini e condizioni comporterà l'avvio di provvedimenti disciplinari da parte del preside e dei Consigli di classe interessati, sulla base del Codice disciplinare d'Istituto. Gli studenti saranno ritenuti responsabili delle loro azioni; sono altresì invitati a segnalare immediatamente ai loro insegnanti ogni uso improprio della rete da parte di terzi (siano alunni, docenti o dipendenti del Collegio).
3. I dispositivi usati impropriamente dagli alunni potranno essere ritirati dal personale docente per l'intera giornata, a tutela del principi contenuti nel presente Regolamento. Se un dispositivo viene ritirato allo studente sarà custodito in segreteria o in presidenza e riconsegnato all'alunno interessato (o ai suoi genitori o responsabili), a discrezione del preside o di un suo delegato, al termine della giornata.

Per quanto non contemplato dai presenti Regolamenti si fa riferimento al Regolamento di Istituto e alle Linee di orientamento MI (Ministero dell'Istruzione) per la prevenzione e il contrasto dei fenomeni di Bullismo e Cyberbullismo, emanate in data 13 gennaio 2021, oltre che all'intero compendio della legislazione vigente.

Il Regolamento informatico d'Istituto – P.U.A. e il BYOD riportati nel presente documento sono stati concepiti dai Collegi docenti d'Istituto; sono stati letti e approvati dagli stessi e sono stati adottati dai Consigli dell'Istituzione delle sedi di Trento e Rovereto con delibera del 23 giugno 2021 e del 24 giugno 2021. A far data da tale validazione, questi documenti costituiscono parte integrante del Regolamento di Istituto e sono riportati nel Sito d'Istituto, per garantirne la massima pubblicità.

Trento, 30 giugno 2021

IL PRESIDE
Paolo Fedrigotti