REGOLAMENTO SERVIZIO RETE WIFI

Regolamento per l'utilizzo e la navigazione

ART 1 – OGGETTO

1.1 – Il presente Regolamento definisce le condizioni generali di utilizzo del servizio di rete WiFi, (denominato "servizio" nel seguito) dell'IIS *L. B. Alberti* di Abano Terme (PD) denominato "Istituto" nel seguito.
1.2 – Il servizio permette la navigazione in Internet all'interno del plesso, utilizzando la tecnologia WiFi.
1.3 – Potranno usufruire del servizio il personale scolastico dell'Istituto.

ART. 2 – REGOLE GENERALI

2.1 – Il servizio è gratuito, senza alcun onere e/o costo di installazione per l'utente; si precisa che resta a carico dell'utente l'onere di dotarsi, a propria cura e spese, della strumentazione tecnica necessaria per usufruire del servizio medesimo, il quale è altresì responsabile del funzionamento degli stessi
2.2 L'Istituto NON FORNISCE NESSUN TIPO DI SUPPORTO ED ASSISTENZA TECNICA agli apparati degli utenti (Pc, smartphone, tablet, ecc.);
2.3 – Il servizio è fornito mediante l'utilizzo di frequenze in banda condivisa e limitata protezione contro interferenza. Pertanto, l'erogazione del servizio e la sua qualità non sono garantite
2.4 – Con il primo utilizzo del servizio l'utente dichiara di aver attentamente letto ed espressamente accettato tutti i termini e le condizioni di utilizzo del servizio medesimo indicati nel presente Regolamento, al quale dovrà attenersi scrupolosamente. Dichiara inoltre di aver preso visione dell'Informativa privacy ai sensi dell'art. 13 del Regolamento EU 679/2016 (GDPR)
2.5 – Il mancato rispetto del Regolamento comporterà immediati provvedimenti che saranno valutati a seconda della gravità dell'azione intrapresa e della sua recidività, fino alla disabilitazione permanente dell'accesso
2.6 – L'utente riconosce che il servizio offerto dall'Istituto non garantisce in alcun modo il contenuto, la qualità, la validità di qualsiasi informazione reperita in rete. Ad ogni modo la rete dell'Istituto dispone di filtri alla navigazione e l'attivazione di firewall al solo scopo di consentire la navigazione verso siti web attinenti e opportuni ad un ambiente scolastico nonché scongiurare rischi di cyberattacco;
2.7 – L'utente prende atto ed accetta l'esistenza del registro dei collegamenti ("log") mantenuto dall'Istituto che adotta misure tecniche ed organizzative necessarie a garantire la riservatezza di tale registro. Il registro dei collegamenti potrà essere esibito solo all'autorità giudiziaria, dietro esplicita richiesta.
2.8 – L'Istituto non sarà responsabile verso l'utente e/o suoi aventi causa e verso terzi per i danni diretti, indiretti o consequenziali che dovessero verificarsi per effetto di sospensioni o interruzioni del servizio
2.9 – L'utente del servizio solleva e manleva l'Istituto da ogni responsabilità per eventuali danni arrecati a terzi nell'ambito del servizio e si assume la piena responsabilità per il contenuto dei messaggi trasmessi.

ART. 3 – MODALITÀ DI ACCESSO AL SERVIZIO

3.1 – L'accesso al servizio è effettuato mediante procedura di autenticazione dei dispositivi in uso agli SSID - Service Set IDentifier - dell'Istituto a seconda della tipologia di utente (Docente, Personale ATA, Studente, Ospite temporaneo).
3.2 – Le credenziali con cui si accede al servizio sono da intendersi personali e non cedibili
3.3 – È responsabilità dell'utente la sicurezza della custodia dei codici di accesso alla rete ed è fatto divieto di comunicarlo esternamente
3.4. Al fine di evitare connessioni automatiche al rilevamento della rete Wi-fi, gli utenti dovranno procedere all'autenticazione ogni qualvolta intendano accedere alla rete.

Firmato digitalmente da STEFANIA PONCHIA

ART. 4 – OBBLIGHI DELL'UTENTE

4.1 – L'utente del servizio è tenuto:

a) ad utilizzare il servizio nel rispetto della legislazione vigente e delle finalità per le quali è stato autorizzato. In particolare, è tenuto ad osservare le leggi vigenti in materia di diritto d'autore e di protezione dei dati personali (D. Lgs. 196/2003 e Reg. EU 679/2016), nonché le specifiche norme relative al settore informatico e delle comunicazioni elettroniche;

b) a non utilizzare il servizio per effettuare comunicazioni che arrechino danni o turbative alla rete o a terzi;

c) a non immettere in rete informazioni che possano presentare forme o contenuti di carattere pornografico, osceno, blasfemo, razzista, diffamatorio o offensivo;

d) a non consentire l'utilizzo, a qualunque titolo, del servizio a terzi, del cui comportamento in rete si assume comunque, ai sensi del presente Regolamento, la responsabilità;

e) ad utilizzare unicamente le risorse per cui il servizio è abilitato: è possibile accedere liberamente ad Internet (Web, Posta elettronica e tutto ciò che è fruibile attraverso la rete), ma non a tutti i possibili servizi esistenti (esempio: programmi per lo scambio di file);

f) a non tentare azioni di scansione della rete o attacchi alla sicurezza, espressamente vietati dalla legislazione vigente;

g) a non utilizzare strumenti (ad esempio sniffer) nelle aree di copertura che potrebbero influenzare negativamente le prestazioni della rete, oltre a violare il diritto alla privacy degli utenti del servizio;

h) a non usare in nessun caso la rete dell'Istituto per scaricare o scambiare materiale illegale. Lo scambio di materiale protetto da Copyright (MP3, film in DivX o DVD, software commerciale, ecc.) è vietato per legge e soggetto a sanzioni penali. In caso di rilevamento di azioni illegali l'Istituto procederà al richiamo formale dell'utente e metterà a disposizione delle autorità che ne facessero richiesta ai sensi di legge tutta la relativa documentazione;

i) a non inviare tramite posta elettronica messaggi pubblicitari e/o promozionali o comunicazioni ad altri utenti e/o gruppi di discussione senza che sia stato richiesto ed ottenuto il relativo consenso ovvero senza che tale invio sia stato sollecitato in modo esplicito;

l) a dotare il proprio PC di adeguate protezioni contro virus e altro genere di intrusioni: l'Istituto non si assume alcuna responsabilità in merito ai dati contenuti nei PC degli utenti del servizio. In caso di aggressione da virus informatico o di attacco da parte di malintenzionati che dovessero in qualsiasi maniera danneggiare l'operatività del PC o i dati in esso contenuti, l'utente non potrà in alcun modo rivalersi sull'Istituto. Si invitano gli utenti a installare sul proprio PC un antivirus efficiente ed aggiornato ed un personal firewall adeguatamente configurato.

Il presente Regolamento è stato approvato con
Delibera n. 46 del Consiglio di Istituto del 11.10.2023

REGOLAMENTO SVOLGIMENTO DEGLI ORGANI COLLEGIALI DI ISTITUTO IN MODALITÀ A DISTANZA

ART. 1 - OGGETTO E RIFERIMENTI NORMATIVI

L'emergenza sanitaria, appena conclusasi, ha permesso di sperimentare alcune pratiche e strumenti legati allo sviluppo delle tecnologie dell'informazione e della comunicazione che potranno mantenere un proprio spazio, sia in eventuali periodi di emergenza sia come strutturale integrazione o alternativa alle modalità tradizionali, **ogni qualvolta se ne ravvisi la necessità**.

Il presente Regolamento intende pertanto disciplinare le modalità di svolgimento delle riunioni collegiali per via telematica, in base all'articolo 40 del testo unico di cui al decreto legislativo 16 aprile 1994, n. 297, nonché in base alle disposizioni vigenti oggi e in futuro relativamente ad emergenze sanitarie o di altra natura.

ART. 2 - DEFINIZIONE

Per "seduta in modalità telematica" si intende la seduta degli Organi Collegiali scolastici, nella quale i componenti partecipano a distanza. La partecipazione on-line, mediante l'uso delle apposite funzioni presenti nella piattaforma telematica Google Workspace for Edu (o altre piattaforme), deve avvenire secondo le modalità di cui ai successivi articoli.

Firmato digitalmente da STEFANIA PONCHIA

ART. 3 - REQUISITI PER LE RIUNIONI TELEMATICHE

La partecipazione a distanza alle riunioni dei suddetti OO.CC. presuppone la disponibilità di strumenti telematici idonei a consentire la **comunicazione in tempo reale a due vie** e, quindi, il collegamento simultaneo fra tutti i partecipanti.

Gli strumenti tecnologici utilizzati per lo svolgimento in via telematica delle sedute degli organi collegiali scolastici, devono assicurare:

- la riservatezza della seduta;
- il collegamento simultaneo tra i partecipanti su un piano di parità;
- la visione degli atti della riunione e/o lo scambio – anche mediante l'invio in data precedente alle sedute degli OO.CC. (mediante avvisi mezzo circolari interne, posta elettronica, registro elettronico e/o sistemi informatici di condivisione dei file, Google form o altri) di documenti pertinenti per le riunioni stesse;
- la sicurezza dei dati e delle informazioni.

Ai componenti è consentito collegarsi da qualsiasi luogo che assicuri il rispetto delle prescrizioni del presente articolo, purché non pubblico né aperto al pubblico.

Nelle riunioni a distanza, ai fini della validità della seduta e delle delibere, devono essere rispettate le prescrizioni contenute nel presente regolamento.

ART. 4 - CONVOCAZIONE DELLE SEDUTE A DISTANZA

Nell'avviso di convocazione (attraverso la pubblicazione sul registro elettronico o attraverso diretto invio agli interessati per posta elettronica), deve essere specificato che la seduta avviene tramite strumenti telematici, indicando la modalità operativa di partecipazione.

La convocazione in modalità on line, deve essere inviata, a cura del Presidente, a tutti componenti dell'organo, di norma almeno 5 giorni prima della data fissata per l'adunanza.

ART. 5 – VALIDITÀ E SVOLGIMENTO DELLE SEDUTE A DISTANZA

Per la validità delle sedute in modalità telematica restano fermi i requisiti di validità richiesti per l'adunanza ordinaria:

- regolare convocazione di tutti i componenti con l'elenco degli argomenti indicati all'o.d.g.
- partecipazione della metà più uno degli aventi diritto (quorum costitutivo). Ai fini della determinazione del menzionato quorum costitutivo, dal numero dei componenti l'organo, si sottraggono coloro che abbiano giustificato con comunicazione scritta la loro assenza;
- raggiungimento della maggioranza dei voti richiesta dalle norme di riferimento (quorum deliberativo).

Nell'ipotesi in cui, all'inizio o durante lo svolgimento della riunione, il collegamento di uno o più componenti risulti impossibile o venga interrotto per problemi tecnici, se il numero legale è assicurato la riunione può comunque svolgersi, dando atto dell'assenza giustificata del/i componente/i impossibilitato/i a mantenere attivo il collegamento.

In caso di problemi di connessione durante una votazione, in mancanza di possibilità di ripristino del collegamento in tempi brevi, il Presidente dell'O.C. dichiara nulla la votazione e dispone l'aggiornamento in data da destinarsi della riunione stessa, eventualmente anche nella forma della consultazione telematica asincrona di cui all'art. 2. In tal caso restano comunque valide le deliberazioni adottate fino al momento della sospensione della seduta.

Preliminarmente alla trattazione dei punti all'ordine del giorno, compete al segretario verbalizzante verificare la sussistenza del numero legale dei partecipanti mediante appello o verificando, attraverso la piattaforma utilizzata, l'indicazione numerica delle persone collegate.

ART. 6 - CONSULTAZIONE TELEMATICA ASINCRONA

Gli Organi Collegiali di Istituto possono essere consultati in modalità telematica asincrona, attraverso l'uso di una piattaforma di comunicazione fornita dall'Istituto stesso.

Il voto elettronico è previsto esclusivamente per l'assunzione di delibere chiaramente formulate e principalmente relative ad aspetti tecnico-esecutivi, al termine di un percorso istruttorio noto. L'avviso della consultazione, corredato dalla necessaria documentazione relativa alle delibere, deve

Firmato digitalmente da STEFANIA PONCHIA

pervenire di norma almeno cinque giorni prima rispetto all'avvio delle votazioni e deve contenere l'indicazione della durata prevista, non inferiore alle 12 ore, e l'esplicita definizione dell'orario di chiusura.
I risultati della votazione saranno considerati validi soltanto se espressi dalla metà più uno dei componenti, verranno ufficialmente comunicati nel giorno successivo alla consultazione e in occasione della seduta successiva.
L'adunanza telematica sarà utilizzata dagli OO.CC. per deliberare sulle materie di propria competenza. Le votazioni a scrutinio segreto avverranno esclusivamente in presenza.

ART. 7 - CONVOCAZIONE TELEMATICA E CONSULTAZIONE SINCRONA DEGLI ORGANI COLLEGIALI AD ECCEZIONE DELCOLLEGIO DEI DOCENTI

Gli Organi Collegiali possono riunirsi anche utilizzando servizi di web conference. In questo caso la convocazione dovrà contenere anche l'indicazione della piattaforma utilizzata, eventuali istruzioni e il link o le credenziali per accedere alla videoconferenza.
In particolare, le votazioni potranno avvenire, in base alla scelta da parte del Presidente, sia a voce che tramite chat o altre forme di interazione sincrona presenti nella piattaforma o allestite dall'Istituto.
Il risultato della votazione sarà considerato valido soltanto se espresso dalla metà più uno dei componenti dell'organo.
Dovrà essere posta particolare attenzione al rispetto del turno di parola e ad eventuali accorgimenti tecnici (ad esempio la chiusura dei microfoni in fase di ascolto) che permettano di migliorare la partecipazione alla seduta. La videocamera dei partecipanti andrà tenuta accesa per tutta la durata della seduta, e non sarà consentito l'utilizzo della chat se non per comunicazioni di servizio.
È fatto assoluto divieto ai docenti ed al Presidente assumere atteggiamenti di scherno e derisione o lesivi dell'onorabilità dei componenti dell'organo collegiale. È consentita l'espressione di giudizi critici, se motivati, sui singoli punti all'o.d.g. fatto salvo il diritto del docente a cui sia stata rivolta una critica di rispondere e far verbalizzare le sue dichiarazioni.

ART. 8 CONVOCAZIONE TELEMATICA E CONSULTAZIONE SINCRONA DEL COLLEGIO DEI DOCENTI

Il Collegio dei Docenti può riunirsi anche utilizzando servizi di web conference, con varie modalità operative per le votazioni delle delibere. In questo caso la convocazione dovrà contenere anche l'indicazione della piattaforma utilizzata, eventuali istruzioni e il link o le credenziali per accedere alla videoconferenza.
Attraverso la piattaforma, la chat integrata nell'ambiente utilizzato per la videoconferenza o altri strumenti espressamente indicati, tutti i membri del Collegio presenti sono tenuti a registrare l'ingresso e l'uscita dall'assemblea ed esprimere il proprio voto, favorevole o contrario, o a palesare la propria astensione.

ART. 9 REGISTRAZIONE DELLA VIDEO SEDUTA DEL COLLEGIO DOCENTI O DEL CONSIGLIO D'ISTITUTO

L'uso della video registrazione della seduta del Collegio Docenti e del Consiglio d'istituto è consentito solo se finalizzato alla redazione del verbale e non anche all'uso personale.
In tal caso, e previa proposta da parte del Presidente, deve essere comunque autorizzato dallo stesso organo collegiale con apposita mozione ad hoc che sarà sottoposta a votazione prima di ogni seduta. È fatto divieto ogni utilizzo difforme alle finalità per la quale è stata autorizzata la registrazione, come per esempio la diffusione o la comunicazione a terzi non autorizzati.

ART. 10 CONDIZIONI DI UTILIZZO DELLA PIATTAFORMA IN USO

I partecipanti agli OO.CC. si impegnano:

- a conservare la password personale e a non consentirne l'uso ad altre persone;
- a comunicare immediatamente l'impossibilità ad accedere al proprio account o il sospetto che altri possano accedervi al coordinatore di classe;
- a non consentire ad altri, a nessun titolo, l'utilizzo della piattaforma Google Workspace for

Firmato digitalmente da STEFANIA PONCHIA

Education;

- a non diffondere eventuali informazioni riservate di cui si venisse a conoscenza, relative all'attività delle altre persone che utilizzano il servizio;
- ad osservare il presente regolamento, pena la sospensione dell'account personale dell'utente;
- ad utilizzare i servizi offerti solo ad uso esclusivo per le attività didattiche della scuola.
- a rispettare le regole del buon costume

Il personale scolastico si assume inoltre la piena responsabilità di tutti i dati inoltrati, creati e gestiti attraverso la piattaforma in uso.

ART. 11 DURATA E DISPOSIZIONI FINALI

Il presente regolamento avrà effetto dalla sua approvazione e fino all'occorrenza di modifiche o integrazioni.

Il presente Regolamento è stato approvato con
Delibera n. 46 del Consiglio di Istituto del 11-10-2023

REGOLAMENTO INTERNO SULL'UTILIZZO DI INTERNET E DELLA CASELLA DI POSTA ELETTRONICA ISTITUZIONALE SUL LUOGO DI LAVORO

IL DIRIGENTE SCOLASTICO

VISTO il Provvedimento del Garante per la Protezione dei Dati Personali 1° marzo 2007 n. 13 (in G.U. n. 58 del 10 marzo 2007);

VISTA la Direttiva del Dipartimento della Funzione Pubblica 26 maggio 2009, n. 2;

VISTO il D.P.R. 16 aprile 2013 n. 62 recante il nuovo Codice di condotta dei dipendenti pubblici e successive modifiche del D.P.R. del 13 giugno 2023, n. 81

VISTO l'art. 92 del CCNL 2007;

CONSIDERATO che l'istituzione scolastica, quale datore di lavoro, in persona del Dirigente Scolastico pro tempore è tenuta ad assicurare la funzionalità ed il corretto impiego degli strumenti ICT da parte dei propri dipendenti, definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa ed adottando le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informativi;

CONSIDERATO che a fronte del potere di controllo dell'Amministrazione datore di lavoro, esiste in capo ai dipendenti l'obbligo, sancito da norme di legge (anche di rilevanza penale) e di contratto, di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa ed idonei a non causare danni o pericoli ai beni mobili ed agli strumenti ad essi affidati, tra i quali vi sono le attrezzature ICT ed i sistemi informativi messi a disposizione dall'Amministrazione;

CONSIDERATO che il datore di lavoro (secondo i poteri a lui affidati dalle norme del codice civile, articoli 2086, 2087 e 2104), può riservarsi di controllare l'effettivo adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di lavoro. Nell'esercizio di tali prerogative, tuttavia, deve rispettare la libertà e la dignità dei lavoratori, tenendo presente, al riguardo, quanto disposto dalle norme poste a tutela del lavoratore;

CONSIDERATO che l'Amministrazione, tenendo conto delle peculiarità proprie di ciascuna organizzazione ed articolazione di uffici ed, eventualmente, anche dei diversi profili professionali autorizzati all'uso della rete, potrà adottare una o più delle misure indicate dalla deliberazione del Garante della privacy 1 marzo 2007 n. 13;

VISTA la Delibera n.46 del Consiglio di Istituto del 11/10/2023
ADOTTA

il presente regolamento, avente ad oggetto la precisa definizione di criteri e modalità di accesso ed utilizzo ai servizi Internet e posta elettronica da parte del **personale dipendente** dell'IIS *L. B. Alberti* di Abano Terme (PD).

Firmato digitalmente da STEFANIA PONCHIA

ART. 1 MODALITÀ DI UTILIZZO DELLE POSTAZIONI DI LAVORO

L'accesso alla rete Internet è concesso ai dipendenti quali utenti autenticati e nei limiti stabiliti per ciascun profilo di utenza, così come indicati nelle relative lettere di incarico e nell'informativa loro rilasciata ai sensi dell'art. 13 del GDPR.
Per accedere ai servizi informatici legati al registro elettronico adottato l'utente deve necessariamente ed obbligatoriamente autenticarsi, utilizzando una login e una password. La scuola ha individuato le modalità relative al rilascio ed alla gestione delle credenziali di autenticazione. La procedura di assegnazione prevede il cambio password obbligatorio al primo accesso e il successivo cambio obbligatorio ogni 90gg. Ogni utente è responsabile per il proprio account e per l'uso che ne viene fatto, essendo tenuto a tutelarlo da accessi non autorizzati. Non è ammessa la comunicazione del proprio account a terzi.
L'utente ha l'obbligo di:

- non cedere, una volta superata la fase di autenticazione, l'uso della propria postazione a persone non autorizzate;
- non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione, provvedendo a bloccare la postazione in caso di allontanamento temporaneo,
- conservare la password nella massima riservatezza e con la massima diligenza;
- non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a persone non autorizzate, in particolar modo per quanto riguarda l'accesso a Internet ed ai servizi di posta elettronica;
- spegnere il PC al termine del lavoro o in caso di assenze prolungate dalla propria postazione;
- prestare la massima attenzione ai supporti di origine esterna (es. pen drive), verificando preventivamente tramite il programma di antivirus ogni file acquisito attraverso qualsiasi supporto e avvertendo immediatamente l'Amministratore di Sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti.

ART. 2 - MISURE DI SICUREZZA PREDISPOSTE DALL'ISTITUZIONE SCOLASTICA

L'utilizzo di Internet è permesso esclusivamente in relazione a finalità istituzionali e connesse all'attività lavorativa.
In ottemperanza al provvedimento del Garante del 01/03/2007, l'Istituzione scolastica ha provveduto ad adottare le seguenti misure organizzative finalizzate alla prevenzione di utilizzi non pertinenti della rete internet:

- individuazione di categorie e liste di siti bloccati (black list) periodicamente aggiornate;
- configurazione di sistemi hardware e software che filtrino i siti ed i servizi non consentiti individuati precedentemente e che prevengono determinate operazioni non correlate all'attività lavorativa.

Per gli utenti che accedono a Internet è vietato:

- reiterare tentativi di accesso a siti bloccati e di cui si è avuta evidenza del fatto che si tratta di siti non appropriati e non consentiti;
- servirsi delle postazioni di accesso a Internet per attività non istituzionali e non connesse ad attività lavorative e per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- registrarsi a siti i cui contenuti non siano connessi all'attività lavorativa;
- accedere a siti pornografici, siti recanti istigazione a violenza e a delinquere in genere, siti di intrattenimento e siti commerciali per operazioni di compravendita;
- utilizzare sistemi di chat non previamente autorizzati e non correlati a finalità istituzionali.

ART. 3 UTILIZZO DELLA POSTA ELETTRONICA

A tutte le componenti scolastiche è assegnato un account di posta elettronica istituzionale legato al dominio dell'Istituto, nel formato: nome.cognome@istitutoalberti.edu.it
L'utilizzo di posta elettronica è consentito **solo per motivi istituzionali** e connessi all'attività lavorativa.

Firmato digitalmente da STEFANIA PONCHIA

L'accesso è consentito in via esclusiva ai dipendenti ai quali sono state comunicate credenziali di autenticazione per l'accesso alla casella di posta. Si precisa che:

- La casella è strettamente personale e non è ammesso l'utilizzo da parte di persone diverse dall'assegnatario, né questi può cederla a terzi.
- L'indirizzo di posta elettronica può essere correlato ad altri servizi come accesso a portali, piattaforme didattiche (es. Google G Suite) e a tutti gli ambienti Internet legati solo ed esclusivamente ad attività lavorative e didattiche (per esempio per consultazione versioni e/o risorse digitali dei libri di testo adottati).
- È vietato trasmettere materiale commerciale e/o pubblicitario non richiesto (spamming), nonché permettere che le proprie risorse siano utilizzate da terzi per questa attività.
- È vietato prendere visione della posta altrui e simulare l'identità di un altro utente, ovvero utilizzare per l'invio di messaggi credenziali di posta non proprie, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza.
- È vietato trasmettere a mezzo posta elettronica dati sensibili, personali o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento della protezione dei dati.

ART. 4 CONTROLLI PREVISTI E SANZIONI

Nel rispetto della normativa vigente richiamata nelle premesse del presente disciplinare, l'istituzione scolastica non procede a verifiche che possano configurare il controllo a distanza dell'attività dei lavoratori.

L'Amministrazione, in persona del dirigente scolastico, si riserva la **facoltà** di eseguire **controlli** in conformità alla legge, sia per eseguire verifiche sulla funzionalità e sicurezza di reti e sistemi, sia per eseguire verifiche sul corretto utilizzo dei servizi Internet e posta elettronica, in conformità a quanto prescritto dal presente disciplinare, dalla normativa posta a protezione dei dati personali.

I controlli sono posti in essere dal Titolare del trattamento dati coadiuvato dall'amministratore di sistema. Ci si potrà avvalere di personale esterno, appositamente nominato quale responsabile esterno di trattamento, secondo le previsioni del reg. EU 679/2016 e s.m.i.

I controlli sono eseguiti tenendo conto del principio di graduazione (par. 6.1 del Provvedimento del Garante per la Protezione dei Dati Personali 1/3/2007) e procederanno come segue:

- al verificarsi di comportamenti anomali, il dirigente deve effettuare: **A.** un controllo anonimo su dati aggregati, riferito all'intera struttura amministrativa oppure a sue aree. Il controllo anonimo potrà concludersi con un avviso generalizzato relativo all'utilizzo anomalo degli strumenti dell'amministrazione e con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite ai dipendenti; in assenza di successive anomalie non si effettueranno controlli su base individuale; **B.** nel perdurare delle anomalie si procederà a controlli su base individuale o per postazioni di lavoro;
- in caso di abusi singoli e reiterati si procederà all'invio di avvisi individuali e si eseguiranno controlli nominativi o su singoli dispositivi e/o postazioni di lavoro;
- in caso di riscontrato e reiterato uso non conforme delle risorse informatiche, verrà attivato il procedimento disciplinare nelle forme e con le modalità di cui al D. Lgs. n. 165 del 2001 articoli 55 bis e seguenti.

Il presente regolamento è stato approvato con
Delibera n. 46 del Consiglio di Istituto del 11-10-2023

REGOLAMENTO BYOD
BRING YOUR OWN DEVICES
Regolamento per l'utilizzo dei dispositivi digitali personali

I. UTILIZZO DI DISPOSITIVI PERSONALI IN SEDE DI DIDATTICA E FORMAZIONE DIGITALE DA PARTE DI ALUNNI E DOCENTI

Le "Politiche attive per il BYOD (*Bring Your Own Device*) dell'IIS *L. B. Alberti* di Abano Terme (PD) prevedono che la scuola riconosca la possibilità per gli **alunni, il personale docente E IL**

Firmato digitalmente da STEFANIA PONCHIA

PERSONALE di una formazione digitale che parta dal saper utilizzare in modo consapevole i propri dispositivi.
Si legge testualmente nel Piano Nazionale: "*La scuola digitale, in collaborazione con le famiglie e gli enti locali, deve aprirsi al cosiddetto BYOD* (Bring Your Own Device)*, ossia a politiche per cui l'utilizzo di dispositivi elettronici personali durante le attività didattiche sia possibile ed efficientemente integrato*".
Pertanto, al fine di offrire agli **alunni e il personale docente** opportunità innovative e inedite per incrementare la loro formazione, il nostro Istituto intende favorire tale processo attraverso una modalità che contribuisca al miglioramento dell'ambiente educativo e di apprendimento garantendone la sicurezza.
È altresì obiettivo di detta azione quello di formare gli **alunni e il personale docente e ATA** a una corretta gestione dei rischi e pericoli della Rete.

Si rende pertanto **necessario normare** l'uso dei dispositivi mobili a scuola:
Dispositivi ammessi: qualsiasi computer portatile, tablet, e-reader, smartphone.

I dispositivi devono essere usati a scuola per soli scopi didattici e solo dopo **previa autorizzazione esplicita** dei docenti i quali amministrano tempi e necessità di utilizzo di tali apparecchiature.

È vietato agli studenti e ai dipendenti usare dispositivi di registrazione audio, videocamere o fotocamere (o dispositivi che li prevedano) per registrare media o fare foto durante le attività scolastiche.
Agli studenti non è permesso usare i dispositivi per giochi durante le ore scolastiche né utilizzare il cellulare per chiamate, sms, o messaggistica in genere. Si ribadisce la puntuale applicazione della normativa vigente (DPR 249/1998, DPR 235/2007, Direttiva Ministeriale 15.03.2007), pertanto l'uso del cellulare in quanto tale non è consentito per ricevere/effettuare chiamate, SMS o altro tipo di messaggistica

Si richiama l'attenzione degli alunni, dei docenti, del personale ATA 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, nei casi più gravi, gli estremi di veri e propri reati. Audio e video registrati a scuola a fini didattici possono essere pubblicati esclusivamente in canali di comunicazione intestati ufficialmente all'IIS *L. B. Alberti* di Abano Terme (PD) da cui potranno essere condivisi.

La comunicazione con le famiglie, per **qualsiasi urgenza**, è sempre garantita attraverso il telefono della scuola. I docenti possono derogare a tali disposizioni, consentendo l'uso del cellulare, in caso di particolari situazioni non risolvibili in altro modo.

Le **famiglie** sono invitate a collaborare strettamente con l'Istituto, nello spirito della corresponsabilità educativa, **evitando ad esempio** di inviare messaggi o effettuare chiamate ai telefoni dei propri figli, durante l'orario scolastico.
Gli **studenti**, così come il **personale**, sono responsabili personalmente dei propri dispositivi; è vietato prendere in prestito dispositivi di altri studenti.
Gli studenti sono responsabili di riportare a casa il dispositivo al termine delle lezioni. La scuola non sarà ritenuta responsabile per nessun dispositivo degli studenti lasciato a scuola.
Agli studenti e al personale docente è richiesto di caricare completamente il dispositivo a casa e devono essere consapevoli che:

- non sarà possibile ricaricare i dispositivi personali durante l'orario di lezione;
- non sarà possibile ricaricare i dispositivi in aula; a tal scopo si consiglia di dotarsi di caricabatteria portatili;
- la scuola non è tenuta a fornire trasformatori di emergenza per ricaricare i dispositivi personali (soprattutto PC portatili)

Firmato digitalmente da STEFANIA PONCHIA

Ogni dispositivo personale (tablet o PC) dovrà essere **contrassegnato** a cura del proprietario, con l'indicazione di nome e cognome.

I docenti dovranno ritirare i dispositivi digitali personali degli studenti a inizio lezione (o in qualsiasi altro momento della lezione stessa) e riconsegnarli a fine lezione o al momento dell'uso didattico degli stessi.
Ogni utilizzo non autorizzato, al di fuori di quanto previsto in precedenza, non è permesso e sarà sanzionato.
La scuola promuove iniziative di informazione e formazione sui temi dell'uso consapevole dei dispositivi informatici, dei nuovi media, dei social network e in generale delle applicazioni web e mobili.

II. NORME SPECIFICHE PER I DISPOSITIVI DIGITALI DI PROPRIETÀ DELLA SCUOLA

L'utilizzo dei dispositivi digitali in dotazione alla scuola è autorizzato dal Dirigente Scolastico.
Il docente che intende usufruire dei pc portatili con la propria classe assegna il laptop all'alunno utilizzatore e compila il registro preposto dove indica la classe, il laptop assegnato ad ogni singolo alunno (rispettando l'ordine alfabetico), la materia trattata, l'orario di utilizzo, la segnalazione di eventuali problemi o danni verificatesi durante la lezione.
L'alunno utilizzatore è tenuto al corretto utilizzo del dispositivo, secondo il buon senso e le indicazioni del docente.
Il docente è tenuto al rapido controllo dei dispositivi all'atto della riconsegna e alla tempestiva segnalazione di eventuali danneggiamenti.

L'utilizzo dei display digitali, del pc presente in ogni aula o nei laboratori è subordinato sempre alla supervisione di un docente.

Uso non consentito di Internet:

- Usare Internet per scopi diversi da quelli didattici;
- Scaricare musica, video e programmi da internet o qualsiasi file senza il consenso dell'insegnante;
- Giocare sul computer, in rete o diversamente (se non come parte di una lezione);

Diritti di proprietà intellettuale
Gli studenti devono rispettare e proteggere la proprietà intellettuale altrui:

- Non è ammessa la copia o il plagio di qualsiasi materiale;
- Non è ammessa la violazione dei *copyrights*;
- Si deve attribuire, citare e richiedere il permesso degli autori o creatori delle informazioni o dei media originali (se richiesto dalla legge o da accordo).

La scuola favorisce e incoraggia lo sviluppo dell'*open source* e *copyleft*

Diritto di ispezione
Per i dispositivi di sua proprietà, l'istituto si riserva il diritto di monitorare le attività online degli utenti e accedere, controllare, copiare, raccogliere o cancellare ogni comunicazione elettronica o file e rivelarli all'autorità giudiziaria e alla famiglia se ritenuto necessario.

Sanzioni per il mancato rispetto del Regolamento
L'accesso alla rete della scuola è un privilegio, non un diritto. L'uso della tecnologia, sia essa di proprietà della scuola o di un dispositivo fornito agli studenti, comporta responsabilità personali. Ci si aspetta che gli studenti rispettino le regole dell'IIS *L. B. Alberti* di Abano Terme (PD), agiscano responsabilmente e rispettino i termini e le condizioni fissate dall'insegnante di classe e dalla scuola. Il mancato rispetto di questi termini e condizioni potrà risultare nella temporanea o permanente perdita di accesso alla rete nonché altre azioni disciplinari e legali, se necessario.

Firmato digitalmente da STEFANIA PONCHIA

Gli studenti saranno ritenuti responsabili delle loro azioni e sono incoraggiati a segnalare immediatamente ogni uso accidentale al loro insegnante o anomalie nella Rete.
Le sanzioni dipenderanno dalla gravità dell'accaduto e saranno comminate secondo il Regolamento di Istituto.
I dispositivi personali potranno essere confiscati per l'intera giornata. Se un dispositivo viene confiscato, verrà depositato presso gli uffici di segreteria per essere riconsegnato ai genitori.

Compiti del Docente
Il Docente ha il compito di sorvegliare costantemente l'attività degli alunni e, se si dovessero verificare episodi di apertura di siti inappropriati durante le attività, gestire con tempestività la loro chiusura e segnalare il fatto all'Assistente Tecnico per effettuare i dovuti controlli sulla macchina affinché non risulti infetta o siano rimaste tracce di navigazioni illecite.

Compito dell'Istituto
Sarà cura della scuola provvedere a mettere a disposizione un adeguato numero di dispositivi, al fine di permettere la partecipazione di tutti gli alunni della classe alle attività programmate dai docenti. L'istituto avrà altresì cura di garantire connessioni sicure mediante l'utilizzo di dispositivi adatti (firewall, parental-control, etc.) compatibilmente con le necessità di utilizzo della Rete e nei limiti dei fondi disponibili.

III. UTILIZZO DI DISPOSITIVI PERSONALI IN REGIME DI "LAVORO AGILE" – P.ATA

Al fine di garantire la sicurezza del trattamento dei dati personali anche con riferimento alle categorie particolari (ex dati sensibili), l'IIS *L. B. Alberti* di Abano Terme (PD) disciplina le modalità di svolgimento del Lavoro Agile estendendo le prescrizioni e le procedure organizzative previste sul luogo di lavoro anche nell'adempimento di attività e mansioni da remoto.

Norme di comportamento per gli assistenti amministrativi al trattamento dei dati
L'incaricato del trattamento è tenuto a prediligere il Lavoro Agile su un terminale fornito direttamente dall'Istituto scolastico, in quanto opportunamente configurato per gestire dati personali in piena sicurezza. Qualora l'istituto non dovesse garantire la consegna di terminali inventariati, si raccomanda l'incaricato di utilizzare il dispositivo personale rispettando le seguenti istruzioni:
1. Assicurarsi di non effettuare forme di salvataggio dati di pertinenza dell'istituto sui propri device;
2. Gestire il proprio lavoro mediante accesso a piattaforme (es. segreteria digitale) e soluzioni di Cloud attivate, evitando l'uso di altre soluzioni di terze parti non espressamente autorizzate dall'Istituto;
3. Limitare l'utilizzo del dispositivo al solo incaricato, evitando durante le attività lavorative la condivisione del terminale con altri soggetti non espressamente autorizzati;
4. Prediligere la navigazione in incognito, al fine di garantire riservatezza qualora il dispositivo fosse soggetto ad uso promiscuo;
5. Su richiesta dell'Istituto è possibile installare software per il "Desktop Remote control" ovvero effettuare accesso ad una VPN;
6. Mantenere attiva l'opzione di aggiornamento automatico del S.O. in uso (Windows, Linux, macOS);
7. Installare un software di protezione antivirus, qualora non fosse già presente, al fine di tutelarsi da potenziali attacchi informatici;
8. Utilizzare sempre e solo indirizzi email con dominio istituzionale, evitando email personali non autorizzate;
9. Predisporre la cifratura dei file (inserimento password) quando la stessa si rende necessaria in ragione della natura dei dati trattati (es. documenti contenenti informazioni particolari dell'utenza come stati di salute ecc…);
10. custodire con la massima diligenza le credenziali di autenticazione (user-id e password) per l'utilizzo del computer e per l'accesso alle banche dati e ai sistemi informativi di competenza;
11. mantenere riservata la propria password evitando qualsiasi forma di condivisione;

Firmato digitalmente da STEFANIA PONCHIA

12. modificare la password almeno ogni sei mesi. Nel caso in cui la password dia l'accesso a dati personali particolari o giudiziari, essa deve essere modificata almeno ogni tre mesi. La password deve essere composta da almeno 8 caratteri (nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito) e non deve contenere riferimenti facilmente riconducibili all'incaricato;
13. presenziare, quando possibile, agli interventi di assistenza e digitare personalmente la propria password. Qualora ciò non sia possibile, provvedere alla modifica alla password immediatamente dopo l'intervento;
14. non collegare modem o dispositivi che consentano un accesso non controllato al computer e alla rete d'Istituto
15. non utilizzare supporti removibili (CD, DVD, PenDrive) di provenienza esterna e, qualora ciò si rivelasse necessario, verificare sempre preliminarmente l'integrità dei supporti con il programma antivirus installato;
16. non scaricare file eseguibili o documenti di testo da siti internet senza verificare l'assenza di virus;
17. non disabilitare la password di screen saver, per evitare accessi non autorizzati quando la postazione non è presidiata;
18. non condividere il proprio hard disk con un altro computer se non in condizioni di protezione da scrittura e con password di accesso;
19. non riutilizzare supporti removibili sui quali siano conservati dati sensibili o giudiziari a meno che i dati in essi contenuti non siano intelleggibili e tecnicamente ricostruibili. Diversamente, i supporti removibili debbono essere distrutti;

Il presente regolamento è stato approvato con
Delibera n. 46 del Consiglio di Istituto del 11-10-2023

Il Dirigente scolastico
Stefania Ponchia
FIRMA AUTOGRAFA SOSTITUITA DA INDICAZIONE A STAMPA
AI SENSI DELL'ART. 3, COMMA 2, DEL D.L. N. 39/93

Firmato digitalmente da STEFANIA PONCHIA