Scuola secondaria di primo grado “Dante Arfelli”
Viale Gastone Sozzi, 6 47042 Cesenatico (FC)
tel. 054780309 - 0547672888 - CF: 90041150401 - CM: FOMM800900A
mail: fomm08900a@istruzione.it - PEC: fomm08900a@pec.istruzione.it
www.smdantearfelli.edu.it

REGOLAMENTO UNIFICATO PER L’UTILIZZO DELLE RISORSE TECNOLOGICHE

SEZIONE I: DESCRIZIONE DELLE RISORSE TECNOLOGICHE E FINALITA’

La Scuola Secondaria di Primo Grado “Dante Arfelli”, nell’ambito del proprio Piano Triennale dell’Offerta Formativa e in coerenza con le indicazioni ministeriali relative all’innovazione didattica e alla transizione digitale, si è dotata di un sistema organizzato e coerente di strumenti tecnologici e ambienti digitali a supporto delle attività educative, organizzative e amministrative.
L’adozione di piattaforme digitali e di dispositivi tecnologici non rappresenta un elemento accessorio, ma costituisce parte integrante del progetto formativo dell’Istituto, orientato allo sviluppo delle competenze digitali, alla promozione di metodologie didattiche collaborative e alla costruzione di ambienti di apprendimento inclusivi, sicuri e innovativi. Le tecnologie vengono utilizzate esclusivamente per finalità didattiche, formative e istituzionali, nel rispetto della normativa vigente.

STRUMENTI DIGITALI ADOTTATI
Tra gli strumenti adottati dall’Istituto riveste un ruolo centrale la piattaforma Google Workspace for Education, ambiente digitale integrato che consente a docenti, studenti e personale scolastico di disporre di account istituzionali nominativi attivati sul dominio scolastico e gestiti internamente da un amministratore di sistema incaricato. Attraverso tali account è possibile accedere ai principali strumenti per la comunicazione e la collaborazione didattica, quali la posta elettronica istituzionale, l’archiviazione e condivisione dei documenti, la gestione delle classi virtuali, la produzione di elaborati digitali, lo svolgimento di videoconferenze in caso di DaD (didattica a distanza). L’ambiente è configurato per uso educativo e sottoposto a controllo amministrativo, in modo da garantire un utilizzo coerente con le finalità scolastiche.
Inoltre, l’Istituto permette a studenti e docenti, di utilizzare, mediante l’account istituzionale e in modo protetto, ulteriori strumenti digitali dedicati alla produzione creativa e multimediale (come Canva in versione educativa, per la realizzazione di presentazioni, elaborati grafici e progetti interdisciplinari), o piattaforme di divulgazione culturale come la biblioteca digitale (MLOL). L’attivazione di queste e altre applicazioni o servizi digitali avviene previa valutazione tecnica e giuridica, con particolare attenzione alla conformità alla normativa in materia di protezione dei dati personali e alle garanzie offerte dai fornitori in termini di sicurezza e trattamento delle informazioni.
L’infrastruttura tecnologica dell’Istituto è costituita da una rete interna protetta, dotata di sistemi di filtraggio della navigazione, firewall e strumenti di protezione perimetrale. Le reti sono organizzate in modo da distinguere gli ambiti didattici da quelli amministrativi e l’accesso ai servizi digitali è regolato mediante credenziali personali e profilate in base al ruolo ricoperto all’interno della comunità scolastica. I dispositivi in dotazione, quali personal computer, lavagne interattive multimediali e strumenti per i laboratori didattici, sono configurati per un utilizzo coerente con le attività educative.

PRIVACY E PROTEZIONE DATI

La protezione dei dati personali rappresenta un elemento prioritario nell'organizzazione digitale della scuola. L'Istituto opera in qualità di Titolare del trattamento dei dati personali e si avvale di un Responsabile della Protezione dei Dati nominato ai sensi del Regolamento (UE) 2016/679. Il trattamento delle informazioni avviene nel rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione, limitazione delle finalità e della conservazione, nonché integrità e riservatezza. I dati trattati negli ambienti digitali scolastici sono limitati a quelli strettamente necessari allo svolgimento delle attività didattiche e istituzionali e comprendono, in particolare, dati identificativi, dati di contatto istituzionali, elaborati prodotti dagli studenti e dati tecnici di accesso utilizzati esclusivamente per finalità di sicurezza informatica.
L'Istituto adotta misure tecniche e organizzative adeguate per garantire un livello di sicurezza proporzionato ai rischi, tra cui aggiornamenti periodici dei sistemi, protezione antivirus e antimalware, procedure di backup e protocolli per la gestione di eventuali incidenti informatici. Gli account istituzionali vengono disattivati al termine del percorso scolastico degli studenti o alla cessazione del rapporto di lavoro del personale, nel rispetto dei tempi di conservazione previsti dalla normativa.
Parallelamente all'implementazione degli strumenti tecnologici, la scuola promuove percorsi di educazione alla cittadinanza digitale, orientati alla consapevolezza nell'uso della rete, alla tutela dell'identità digitale e alla protezione dei dati personali. L'obiettivo è quello di accompagnare studenti e personale in un utilizzo responsabile e maturo delle tecnologie, valorizzandone le potenzialità educative in un contesto sicuro e regolamentato.

ART 1 - OBIETTIVI

1. Il presente regolamento comprende il piano per la sicurezza informatica disciplinando l'accesso e l'uso della rete internet scolastica, l'uso delle piattaforme di E-learning approvate dalla scuola e l'utilizzo dei dispositivi informatici dell'Istituto.
2. l'obiettivo del presente regolamento è quello di favorire una didattica cooperativa e laboratoriale, incentrata sullo sviluppo delle competenze, come previsto dal Piano Nazionale della Scuola Digitale.

ART 2 - AMBITO DI APPLICAZIONE

1. Il presente regolamento si applica a docenti, studenti, personale scolastico nell'ambito delle attività didattiche e amministrative.

ART 3 - PRINCIPI GENERALI

1. L'utilizzo delle risorse tecnologiche è ammesso esclusivamente per la didattica, le funzioni docente, le funzioni strumentali e per le attività amministrative.
2. L'impiego delle risorse tecnologiche deve rispettare i principi di
   - trasparenza e correttezza
   - imparzialità e non discriminazione
   - sicurezza digitale
   - inclusione e accessibilità

ART 4 - DEFINIZIONI

Nel presente Regolamento i termini qui sotto elencati hanno il seguente significato:

1. *Istituto*: Scuola secondaria di primo grado "Dante Arfelli", Cesenatico, Via Sozzi n 6.

2. *Amministratore di sistema*: il responsabile incaricato dalla Dirigente Scolastica per l'amministrazione del servizio di connessione e dei servizi Google e App Web.

3. *Servizio Google*: Servizi digitali integrati in ambiente cloud, erogati dal fornitore Google, finalizzati alla comunicazione, collaborazione, produzione documentale e gestione delle attività didattiche e istituzionali, accessibili tramite account nominativi attivati sul dominio

scolastico. Comprendono i servizi principali (Core Services: drive, gmail, classroom, meet, calendar, etc.), servizi autonomi standalon (Gemini e NotebookLM) e, ove abilitati dall'Istituto, eventuali servizi aggiuntivi (Additional Services).

4. *App Web*: Servizio applicativo cloud fornito da soggetto terzo rispetto all'Istituto, e integrabile con l'ambiente digitale istituzionale del fornitore.

5. *Google*: Google Inc. con sede in 1600 Amphitheatre Parkway Mountain View, CA 94043.

6. *Fornitori di App Web*: tutti i soggetti giuridici elencati nel registro dei trattamenti dell'istituzione scolastica e che forniscono un servizio digitale

7. *Utente*: colui che utilizza un account del servizio Google o che fruisce del servizio di connettività.

8. *Account*: insieme di funzionalità, applicativi, strumenti e contenuti attribuiti ad un nome utente con credenziali di accesso.

9. *Rete Scolastica*: l'insieme coordinato di infrastrutture hardware e software dell'Istituto, predisposte per garantire l'accesso sicuro degli utenti autorizzati, tramite rete cablata (LAN) o wireless (Wi-Fi), ai servizi digitali interni e, l'accesso regolamentato alla connettività internet verso il web, nel rispetto delle misure di sicurezza informatica adottate dall'Istituto.

10. *Attrezzature*: l'insieme di tutti gli strumenti digitali presenti a scuola (PC di ogni grandezza e tipologia, Tablet, ActivBoard, LIM, stampanti)

SEZIONE II: ACCESSO E USO DELLA RETE INTERNET DI ISTITUTO

ART 5 - Descrizione del servizio

L'istituto mette a disposizione dei propri dipendenti e studenti, e degli ospiti, l'accesso alla rete scolastica, al fine di promuovere l'innovazione didattica e migliorare l'efficienza dei servizi amministrativi. La presente sezione disciplina le condizioni di utilizzo della rete scolastica e delle risorse ad essa connesse e definisce le modalità di accesso per la fruizione del servizio.

ART 6 - Gestione del servizio

1. la Rete Scolastica è gestita da un tecnico informatico dipendente dell'amministrazione, appositamente nominato come Amministratore di sistema, che sovrintende alla gestione e manutenzione della rete.
2. L'Amministratore di sistema è
    a. responsabile della sicurezza della Rete Scolastica,
    b. autorizzato a monitorare accessi e traffico,
    c. incaricato a prestare assistenza tecnica agli utenti.

ART 7 - Modalità di Accesso

L'accesso avviene esclusivamente tramite le password fornite dall'Amministratore di Sistema annualmente, comuni a tutto l'istituto e differenziate tra personale, alunni e ospiti.

ART 8 - Postazioni autorizzate

L'uso della rete è consentito nelle seguenti postazioni:

1. **Personale Docente e Ospiti:** dai PC in aula, nei laboratori, nelle sale insegnanti e dai dispositivi personali tramite Wi-Fi istituzionale.
2. **Personale ATA:** dai PC degli uffici e di locali specifici.
3. **Studenti:** dai PC nelle aule e dei laboratori mobili o fissi, sempre e solo con il consenso e sotto la supervisione dei docenti, nei limiti di riservatezza indicati nel regolamento di istituto. Dai device personali consentiti dalle normative vigenti o previsti dal regolamento di disciplina

ART 9 - Responsabilità connesse al servizio

1. Le password non possono essere divulgate al di fuori della scuola o usate da utenti diversi da quelli destinatari, per non incorrere in un Data Breach
2. L'utente è responsabile di tutte le attività svolte durante la sessione di connessione.
3. L'utente, che intende connettersi al servizio con dispositivi personali, deve garantire l'assenza di virus e malware su tali dispositivi

ART 10 - Attività consentite

Per il personale e ospiti:

1. Attività connesse alla propria mansione e strettamente legate all'attività lavorativa
    - Consultazione e gestione della casella di posta istituzionale secondo le indicazioni presenti nel regolamento di istituto
    - Utilizzo del servizio google e delle app web per la didattica e l'amministrazione
    - navigazione in rete inerente all'attività lavorativa
    - A ospiti ed esperti, è consentito l'accesso temporaneo e limitato alle attività didattiche espletate

2. Per gli studenti:
   Fermo restando che ogni attività svolta sulla rete scolastica può essere effettuata solo sotto la supervisione dei docenti, nei limiti di riservatezza indicati nel regolamento di istituto, sono consentite:
    - Le attività didattiche e l'accesso a piattaforme e servizi digitali
    - Utilizzo della posta elettronica istituzionale secondo il presente regolamento

ART 11 - Attività vietate

È espressamente vietato a tutti gli utenti:

1. Accedere alla rete da aree esterne non di pertinenza della scuola
2. Accedere a siti con contenuti pornografici, violenti, o comunque non pertinenti alle attività istituzionali
3. Utilizzare piattaforme di streaming non autorizzate
4. Scaricare o condividere materiale protetto da diritto d'autore
5. Svolgere attività che violino la privacy degli utenti o le disposizioni di legge
6. Utilizzare la rete per attività commerciali o personali
7. Modificare le configurazioni di rete o di sistema delle postazioni.

SEZIONE III: UTILIZZO DELLE PIATTAFORME DI E-LEARNING

ART 12 - Descrizione del servizio

L'istituto mette a disposizione dei propri dipendenti e studenti, un sistema organizzato e coerente di strumenti tecnologici e ambienti digitali a supporto delle attività educative, organizzative e amministrative. Il servizio si compone della piattaforma Google Workspace for Education e degli strumenti digitali e app web in esso integrati o ad esso connessi nei limiti imposti dalla DPIA.

ART 13 - Gestione del servizio

1. Il servizio Google è gestito dal tecnico informatico dipendente dell'amministrazione, appositamente nominato come Amministratore di sistema, che sovrintende alla gestione e manutenzione del servizio.
2. L'amministratore di sistema è responsabile del monitoraggio del Servizio Google e della corrispondente assistenza tecnica agli utenti.

ART 14 - Modalità di Accesso

1. Ogni utente, dopo aver accettato e sottoscritto il presente regolamento attraverso la compilazione e la consegna in segreteria del modulo predisposto, riceve dall'istituto le credenziali personali (mail istituzionale e password) per l'accesso al servizio. Le credenziali rimarranno attive fino al termine dell'attività lavorativa presso l'Istituto.
2. Per ogni studente la creazione dell'account e delle relative credenziali è subordinata all'autorizzazione da parte di uno dei genitori, sempre mediante il modulo predisposto dall'istituto.
3. Le credenziali rilasciate al punto uno e due danno automaticamente accesso anche alle Web App integrate nel servizio Google.
4. L'utilizzo dell'account subirà delle restrizioni dopo 60 giorni dal termine del percorso di studi presso l'Istituto per gli studenti, e dal termine del rapporto lavorativo per i docenti assunti a tempo indeterminato e determinato. L'account verrà poi rimosso definitivamente un anno dopo il termine degli studi o del rapporto di lavoro. Pertanto ogni utente deve provvedere a scaricare e salvare, dal proprio account istituzionale, i materiali e i file di interesse entro tale periodo.

ART 15 - Postazioni autorizzate

L'uso del servizio Google e delle Web App è consentito dalle seguenti postazioni:

4. **Personale Docente:** dai PC in aula, nei laboratori, nelle sale insegnanti e dai dispositivi personali tramite Wi-Fi istituzionale.
5. **Personale ATA:** dai PC degli uffici e di locali specifici.
6. **Studenti:** Durante le attività scolastiche in presenza, sia dai PC nelle aule e dei laboratori mobili e fissi, sia dai device personali (consentiti dalle norme vigenti o previsti dal regolamento di disciplina) o dai device in comodato d'uso,e in ogni caso con la supervisione dei docenti, nei limiti di riservatezza indicati nel regolamento di istituto. Al di fuori delle attività scolastiche in presenza, da device personali o in comodato d'uso e sotto la supervisione dei genitori.

ART 16 - Responsabilità connesse al servizio

1. L'utente si assume la piena responsabilità di tutti i dati inoltrati, creati e gestiti attraverso il servizio Google o le App web, e accetta di essere riconosciuto quale autore dei messaggi inviati e ricevente dei messaggi spediti al suo account.
2. L'utente è responsabile delle azioni compiute tramite il suo account ed esonera l'istituto da ogni pretesa o azione che dovesse essere rivolta all'istituto medesimo da qualunque soggetto, in conseguenza di un uso improprio del servizio.
3. E' responsabilità dell'utente conservare la password personale e in caso di smarrimento delle credenziali rivolgersi direttamente all'amministratore del sistema o, per gli studenti, al coordinatore della classe
4. L'utente deve comunicare immediatamente all'amministratore di sistema o, per gli alunni, al coordinatore di classe l'impossibilità ad accedere al proprio account o il sospetto che altri possano accedervi;

5. L’utente deve rispettare le regole che disciplinano il comportamento nel rapportarsi con gli altri utenti e a non ledere i diritti e la dignità delle persone. In particolare, gli alunni devono essere rispettosi nel rivolgersi ai compagni ed al personale scolastico utilizzando un linguaggio corretto ed appropriato ad un ambiente ove si svolgono attività didattiche;
6. L’utente è tenuto ad osservare le indicazioni in appendice sulla gestione dei dati personali.
7. Il personale si impegna a consultare la propria casella di posta istituzionale come da regolamento di istituto.

ART 17 - Attività vietate

ogni utente si impegna a:

1. Non comunicare né cedere, per nessun motivo, le proprie credenziali di accesso al servizio Google ad altre persone, configurandosi tale azione come un Data Breach (violazione dei dati personali)
2. Non commettere tramite il servizio fornito, violazioni della legislazione vigente, del regolamento d'istituto e di qualsiasi ulteriore regolamentazione deliberato dagli organi dell’istituto.
3. Non consentire ad altri, a nessun titolo, l'utilizzo del Servizio Google e delle App Web tramite le proprie credenziali.
4. Non utilizzare credenziali di altri utenti per accedere ai servizi disciplinati da questo regolamento
5. Non utilizzare il servizio per gestire e divulgare dati personali anche di terze persone.
6. Non utilizzare i servizi per compiere azioni e/o comunicazioni che arrechino danni o turbative alla rete o a altri utenti, o che violino le leggi ed i Regolamenti d’istituto.
7. Non trasmettere o condividere informazioni che possano presentare forme o contenuti di carattere osceno, blasfemo, diffamatorio o contrario all’ordine pubblico alle leggi vigenti in materia civile, penale ed amministrativa.
8. Non immettere in rete materiale che violi diritti d’autore, o altri diritti di proprietà intellettuali o industriali o che costituisca concorrenza sleale.
9. Non fare pubblicità,
10. Non trasmettere o rendere disponibile, attraverso il proprio account, qualsiasi tipo di software, prodotto o servizio che violi il presente Regolamento o la legge vigente.
11. Non modificare i parametri di condivisione e l’organizzazione di cartelle e file predisposti dall’istituto

ART 18 - RISERVATEZZA DEI DATI PERSONALI

1. L’istituto si avvale del servizio offerto dal Fornitore. Pertanto l’istituto non ha alcun ruolo nel garantire la riservatezza dei dati.
2. L’istituto si impegna ad utilizzare i dati relativi all’utente nel rispetto del D.Lgs. 196/2003 del Regolamento (UE) 2016/679, ai soli fini della creazione e mantenimento dell’account.
3. Il servizio è erogato dal fornitore che applica la propria politica alla gestione della privacy; l’utente può conoscere in dettaglio tale politica visitando il sito web di Google e dei fornitori delle singole App Web.

ART 19 - BACKUP E CONSERVAZIONE DEI DATI

1. L'utente solleva l’istituto da ogni responsabilità ed obbligazione in relazione alla cancellazione, al danneggiamento, o alla mancata conservazione dei contenuti nonché al mancato invio/ricezione di messaggi di posta (email).
2. L’istituto si avvale del servizio di backup offerto dal Fornitore. Pertanto l’istituto non ha alcun ruolo nel garantire la conservazione e il recupero del materiale digitale.

ART 20 - GESTIONE DEGLI INCIDENTI INFORMATICI

1. L'Istituto non si ritiene responsabile di eventuali danni arrecati a causa di guasti e/o malfunzionamenti del servizio.
2. Tutti gli utenti si impegnano all'utilizzo responsabile delle risorse a disposizione, affinché la condivisione delle stesse possa contribuire al successo formativo, alla crescita del bagaglio di conoscenze e competenze di ciascuno.
3. L'utente si impegna a comunicare ogni incidente informatico all'Amministratore di sistema o all'animatore digitale. Se l'utente è uno studente, la comunicazione va fatta al coordinatore della classe.

SEZIONE IV: USO DEI SISTEMI INFORMATICI E DOTAZIONI HARDWARE

ART 21 - Descrizione del servizio

L'istituto mette a disposizione dei propri dipendenti e studenti, e di altre figure autorizzate a interventi didattici/educativi, le attrezzature digitali a supporto delle attività educative, organizzative e amministrative, distribuite nelle aule e negli ambienti dell'istituto. Vengono anche messe a disposizioni attrezzature per il comodato d'uso sia a favore degli alunni che dei docenti.

ART 22 - Gestione del servizio

1. Le Attrezzature dell'istituto sono gestite dal tecnico informatico nominato dalla provincia e dalla commissione tecnica informatica appositamente nominata all'interno del corpo docenti.
2. Tecnico e commissione sovrintendono alla gestione e manutenzione del servizio; all'aggiornamento e alla sostituzione dell'attrezzatura, all'assistenza tecnica agli utenti.

ART 23 - Modalità di Accesso

l'accesso alla strumentazione digitale presente nelle aule, se non diversamente indicato dall'amministrazione mediante circolare, è sempre consentito durante tutto l'anno scolastico eccetto nei periodi di chiusura della scuola.
Aule informatiche, Aule mobili (carrelli) e strumentazione digitale presente nei laboratori della scuola, sono accessibili mediante prenotazione con le modalità indicate dall'istituto. Nei periodi di sospensione delle lezioni, è consentito utilizzare la strumentazione digitale solo se previsto all'interno di progetti.
Gli spazi delle aule informatiche, dei laboratori e gli stessi carrelli sono accessibili con apposite chiavi custodite e gestite dal personale individuato annualmente all'interno dell'istituto.

ART 24 - Postazioni autorizzate

E' possibile utilizzare gli strumenti digitali nelle aule, nei laboratori, nelle zone di studio e negli ambienti della segreteria e dei docenti. In ogni altro luogo interno ed all'esterno, è possibile usarli solo con autorizzazione scritta da parte dell'istituto o in caso si tratti di strumenti in comodato d'uso.

ART 25 - Responsabilità connesse al servizio

1. L'utente è responsabile dello strumento che usa.
2. L'utente è tenuto a informare tempestivamente i tecnici di ogni malfunzionamento o incidente sia fisico che data-bleach.
3. l'utente è responsabile di ogni danno arrecato che non sia stato tempestivamente riferito ai tecnici.
4. l'utente è responsabile dello strumento dal momento in cui lo prende al momento in cui lo ripone al suo posto. E' quindi responsabile della sua custodia e dell'eventuale smarrimento dovuto ad abbandono.

5. l’utente è responsabile del materiale digitale salvato sullo strumento digitale (materiale offensivo, etc).
6. In caso di lavoro da remoto o Didattica a Distanza, l'utente deve garantire la riservatezza dei dati nell'ambiente domestico. Si raccomanda pertanto, la creazione di un account utente separato per le attività lavorative, l’uso di una rete protetta da password robusta e crittografia WPA2 o superiore.

ART 26 - Attività consentite

1. Gli strumenti digitali della scuola sono utilizzabili esclusivamente per le attività didattiche le attività amministrative e le attività funzionali all’insegnamento.
2. Al termine dell'utilizzo, l'utente deve effettuare il logout e bloccare la postazione o spegnere il PC per impedire accessi indebiti.
3. è consentito collegare periferiche personali (USB, hard disk, smartphone) ai devices, dopo essersi accertati anche con scansioni antivirus, dell’assenza di virus e malware.

ART 27 - Attività vietate

1. È vietato installare software senza autorizzazione dell'Amministratore di Sistema.
2. I software di protezione (antivirus, firewall) non devono essere disattivati.
3. E’ vietato spostare PC e altri dispositivi facilmente movibili dagli ambienti in cui si trovano. Eventuali necessità in tal senso devono essere preventivamente concordate con i tecnici o se risulta come esigenza continuativa, concordata con l’istituto tramite le modalità indicate dall’istituto

ART 28 - RISERVATEZZA DEI DATI PERSONALI

L'utente solleva l’istituto da ogni responsabilità sulla custodia e protezione di dati personali (password, dati sensibili, documenti personali) salvati nei dispositivi digitali messi a disposizione dall’istituto.

ART 29 - BACKUP E CONSERVAZIONE DEI DATI

1. L'utente solleva l’istituto da ogni responsabilità ed obbligo in relazione alla cancellazione, al danneggiamento, o alla mancata conservazione dei contenuti salvati sui dispositivi della scuola.
2. Non sono previste attività di backup e di ripristino da parte dell’istituto. L’utente provvederà per proprio conto alla realizzazione delle copie di sicurezza che ritenesse necessarie.

ART 30 - GESTIONE DEGLI INCIDENTI INFORMATICI

4. L’Istituto non si ritiene responsabile di eventuali danni arrecati a causa di guasti e/o malfunzionamenti del servizio.
5. Tutti gli utenti si impegnano all’utilizzo responsabile delle risorse a disposizione, affinché la condivisione delle stesse possa contribuire al successo formativo, alla crescita del bagaglio di conoscenze e competenze di ciascuno.

SEZIONE V: MONITORAGGIO, PRIVACY E SANZIONI

ART 31 - FORMAZIONE E SENSIBILIZZAZIONE

L’istituto organizza e svolge annualmente corsi di aggiornamento sull’utilizzo delle dotazioni tecnologiche. Inoltre rilascia a inizio anno a tutto il personale i documenti necessari per un corretto utilizzo degli strumenti tecnologici.

ART 32 - INFRAZIONI E SANZIONI

1. L’istituto tramite l'Amministratore di sistema e i tecnici può monitorare le attività svolte sui servizi descritti nelle sezioni precedenti, per garantire la sicurezza e il rispetto del presente regolamento.
2. In caso di violazione delle norme stabilite nel presente Regolamento, l’Istituto potrà sospendere o revocare l'accesso alla rete o all’account dell’utente, in modo definitivo, senza alcun preavviso e senza alcun addebito a suo carico e fatta salva ogni altra azione di rivalsa nei confronti dei responsabili di dette violazioni.
3. Applicare le sanzioni disciplinari previste dal regolamento di disciplina.
4. Segnalare alle autorità competenti eventuali attività che configurano illeciti civili o penali (es. accesso abusivo, diffusione dati senza autorizzazione, pirateria).
5. L'utente può essere chiamato a rispondere di danni erariali, patrimoniali o d’immagine causati da negligenza grave o dolo nell'uso delle risorse ICT.
6. È obbligatorio segnalare tempestivamente al Dirigente o all'Amministratore ogni sospetta violazione della sicurezza, furto di dispositivi o potenziale data breach.
7. Il presente Regolamento unificato è attuato in stretta conformità con le misure di sicurezza tecniche e organizzative individuate nella DPIA d'Istituto. Qualsiasi comportamento non conforme alle specifiche tecniche della DPIA, anche se non espressamente sanzionato nel presente testo, costituisce violazione disciplinare.

ART 33 - NORME DI SICUREZZA INFORMATICA

1. Password e Credenziali:
    - Utilizzare password di almeno nove caratteri
    - Combinare caratteri alfabetici, numerici e caratteri speciali
    - Evitare riferimenti personali (nome, cognome, date di nascita)
    - Non utilizzare la stessa password per servizi diversi
    - Modificare le credenziali con cadenza trimestrale
    - Non memorizzare le password sui dispositivi o browser
    - Non lasciare le password incustodite
    - Non condividere mai le proprie credenziali
    - Disconnettere ogni volta l’account dai dispositivi comuni

2. Uso della Posta Elettronica:
    - Non aprire allegati da mittenti sconosciuti
    - Verificare la legittimità dei mittenti che sembrano istituzionali
    - Non cliccare su link sospetti
    - Non utilizzare la mail istituzionale per servizi non lavorativi
    - Segnalare immediatamente attività sospette
    - Nell’oggetto della mail non inserire riferimenti a nomi e cognomi

3. Utilizzo dei Dispositivi:
    - Utilizzare solo sistemi operativi con supporto attivo
    - Eseguire scansioni antivirus sui dispositivi esterni
    - Effettuare sempre il logout dai servizi al termine dell'utilizzo
    - Non lasciare incustodite le postazioni sbloccate

4. Sicurezza della Rete:

- Utilizzare solo connessioni Wi-Fi protette
- Non modificare le configurazioni di rete impostate
- Segnalare anomalie all'amministratore di sistema
- Non utilizzare reti Wi-Fi non sicure

5. Gestione dei Dati:
   - Non memorizzare dati personali sui dispositivi della scuola
   - Segnalare immediatamente potenziali violazioni dei dati (data breach)
   - Utilizzare solo dispositivi di archiviazione esterni verificati
   - Effettuare scansioni antivirus prima di collegare dispositivi esterni

ART 34 - SEGNALAZIONE INCIDENTI

Gli utenti sono tenuti a segnalare immediatamente, con le modalità indicate dall'istituto, al dirigente scolastico e ai tecnici:

- Sospette violazioni della sicurezza
- Accessi non autorizzati
- Furti o perdite di dispositivi
- Anomalie nel funzionamento dei sistemi
- Potenziali violazioni dei dati personali (data breach)

In caso di dubbi su attività da effettuare sui sistemi informatici o in caso si sospettino violazioni, gli utenti devono rivolgersi all'Amministratore di sistema o ai tecnici.

ART 12 - NORME FINALI

Il presente regolamento si integra con gli altri regolamenti dell'istituto. L'istituto si riserva il diritto di modificare questo regolamento in qualsiasi momento, dandone comunicazione agli utenti.
Per quanto non espressamente previsto si rimanda alla normativa vigente.

ART 13 - ENTRATA IN VIGORE

il regolamento entra in vigore dopo l'approvazione degli organi competenti ed è soggetto a revisioni periodiche

APPENDICE A: GESTIONE DEI DATI PERSONALI

1. Riservatezza e Trattamento dei Dati (Privacy)
   - L'Istituto si impegna a tutelare i dati personali nel rispetto del Regolamento (UE) 2016/679 (GDPR) e del D.Lgs. 196/2003.
   - L'istituto e il personale trattano i dati personali esclusivamente per finalità istituzionali e per la creazione/mantenimento degli account didattici.
   - Gli alunni non possono trattare dati personali di terze parti
   - Per il servizio google e le app web, l'istituto limita la riservatezza dei dati, gestiti direttamente dai fornitori esterni, alle condizioni contrattuali dei fornitori.
   - Il personale in lavoro agile deve assicurare che terzi non possano visionare dati scolastici riservati nell'ambiente domestico.

2. Monitoraggio della Rete e dei Sistemi
   L'Istituto adotta misure di monitoraggio per garantire la sicurezza delle infrastrutture e la continuità del servizio.

- Controlli: Non vengono effettuati controlli massivi, prolungati o indiscriminati sull'attività online o sulla corrispondenza. È vietato l'uso di strumenti occulti (spyware/keylogger) per la sorveglianza del lavoratore.
- Log di Sistema: I sistemi registrano automaticamente i log di navigazione e accesso (IP, orari, destinatari email) per fini di sicurezza informatica. La consultazione dei suddetti log è consentita solo in caso di anomalie, sospetti di illeciti o violazioni del regolamento, previa autorizzazione del Dirigente Scolastico.