BELLUZZI - FIORAVANTI
ISTITUTO DI ISTRUZIONE SUPERIORE
C.F. 91337340375
via G.D. Cassini,3 - 40133 BOLOGNA
Tel. 051 3519711 - FAX 051 563656
www.iisbelluzzifioravanti.gov.it - bois02300g@istruzione.it

REGOLAMENTO PRIVACY

1 SCOPO E INTRODUZIONE

Ai sensi del Regolamento Europeo 679/2016 e della normativa in vigore volta alla tutela dei dati personali, questo documento ha lo scopo di fornire alle persone designate e autorizzate al trattamento dei dati personali all'interno dell'istituzione scolastica nonché ad alunni e famiglie, informazioni circa:

- Norme comportamentali per un corretto utilizzo dei dati personali, delle attrezzature/supporti, delle tecnologie informatiche e risorse di questo istituto e private utilizzate per trattare dati personali per scopi didattici e professionali;
- Istruzioni per la corretta adozione di misure di prevenzione e per la rilevazione e gestione di problematiche connesse ad un uso non consapevole/non adeguato di dati personali;
- Responsabilità e obblighi spettanti per garantire la protezione e la sicurezza del dato personale (es. relativo a personale scolastico, alunni, personale esterno, ecc.);

2 A CHI È RIVOLTO IL REGOLAMENTO PRIVACY?

Questo regolamento si applica a tutta la comunità della presente comunità scolastica e in particolare:
• ai bambini e ragazzi frequentanti;
• a tutti i docenti che svolgono la loro attività di insegnamento nella nostra scuola;
• al dirigente scolastico e al dirigente dei servizi amministrativi;
• a tutto il personale amministrativo e a tutti i collaboratori scolastici indistintamente;
• a tutti gli operatori/professionisti e/o volontari (a titolo di esempio: educatori, esperti di progetto, ecc…);
• ai genitori tutti;
• ai visitatori/ospiti;
• a tutti coloro che hanno accesso ai sistemi di connessione e usano qualsiasi strumentazione digitale della scuola o anche device personali (dispositivi destinati soprattutto alla navigazione in Internet e pensati soprattutto per un pubblico non professionale) all'interno e al di fuori l'istituto scolastico;

3 DOVE POSSO TROVARE IL REGOLAMENTO PRIVACY?

Il Regolamento Privacy sarà comunicato all'interno della comunità scolastica:
● sul sito della scuola;
● nelle bacheche delle classi e negli spazi pubblici (atrio);
Per il nuovo personale e i nuovi alunni sarà comunicato insieme a tutti i documenti da sottoscrivere all'atto della stipula del contratto/iscrizione.

4 DEFINIZIONI

Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Dati particolari (ex dati sensibili)	Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
Dati giudiziari	I dati personali idonei a rivelare provvedimenti giudiziari;
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; (**il Titolare del trattamento è il presente Istituto Scolastico**);
Interessato	Persona fisica o giuridica, ente o associazione cui si riferiscono i dati personali (**es. gli alunni, il personale docente, ecc**);
Destinatario	La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi;
Consenso dell'interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
Violazione dei dati personali (data breach)	La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
Terzo» (ex incaricato al trattamento – persona autorizzata al trattamento)	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile; (**es. personale scolastico, alunni, docenti, ecc**.)

5 MONITORAGGIO DELL'IMPLEMENTAZIONE DEL REGOLAMENTO PRIVACY E SUO AGGIORNAMENTO.

Il Regolamento Privacy sarà riesaminato annualmente e/o quando si verificheranno cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola. Sarà rivisitato in relazione ad eventuali modifiche organizzative e/o cambiamenti del panorama legilsativo.

6 ISTRUZIONI PER LA CORRETTA GESTIONE E PROTEZIONE DEL DATO PERSONALE

6.1 GESTIONE ACCESSI E UTILIZZO ATTREZZATURE

- Ogni utente si impegna a non cedere a nessuno le proprie credenziali/password (ad esempio nessuno dovrebbe accedere con un nome utente non suo ai servizi, evitare che gli studenti siano in possesso dei dati di login degli insegnanti e del personale scolastico, ecc.)
- Ogni utente si impegna a non abbandonare la propria postazione di lavoro senza aver spento/disconnesso il pc o aver inserito uno screen saver con password (ad esempio evitare di lasciare sessioni aperte per errore da utenti precedenti: in questo caso uscire dalla sessione e informare l'utente;
- Ogni utente è autorizzato ad utilizzare qualsiasi computer, portatile e attrezzatura in prestito dalla scuola a fini esclusivamente a professionali e/o didattici;
- Ogni utente deve avere cura delle attrezzature in dotazione segnalando tempestivamete eventuali problemi al Dirigente Scolastico e/o al persona tecnico competente ove presente (es. malfunzionamenti, virus, ecc.) usando i sistemi di difesa e antivirus;
- Alla verifica di un malfunzionamento del PC o in presenza di una violazione dei dati personali (es. diffusione di una foto via internet o sul sito dell'istituto senza consenso) o qualsiasi altra casistica che può far sospettare "data breach" (violazione di dati personali) o altra minaccia (es. la presenza di un virus che infetta un pc), l'utente deve:
    1. Contattare immediatamente il docente/responsabile di area/collaboratore tecnico;
    2. Sospendere ogni operazione sul PC/dispositivo utilizzato evitando di lavorare con il sistema infetto;
- Ogni utente non consente ad alcuna fonte esterna di accedere in remoto alla propria rete salvo presenza di una chiara necessità professionale;
- Nessun elemento personale può essere aggiunto al dispositivo in dotazione senza previa autorizzazione da parte della Dirigenza (ad es. scaricare software senza adeguata e valida licenza o altri tipi di risorse da Internet che possono in qualche modo compromettere la rete interna della scuola o che possono bypassare i filtri e i sistemi di sicurezza, non modificare le configurazioni impostate sul proprio PC o rete di istituto, ecc.)
- Si invita il personale scolastico e gli alunni a fare attenzione in caso di apertura di file e allegati "sospetti" e di fare attenzione in caso di collegamenti di memorie esterne (es. controllare sempre la presenza o meno di virus ecc.)

- Il personale scolastico, nell'ambito delle proprie mansioni, ha il compito di salvaguardare il comportamento degli alunni verificando che l'accesso degli studenti avvenga sempre e solamente sotto la propria supervisione e unicamente con gli strumenti messi a disposizione dalla scuola;
- Gli alunni sono tenuti a utilizzare l'attrezzatura messa a disposizione dall'istituzione scolastica (LIM presenti nelle classi, PC portatili, tablet, notebook, ecc.) sempre sotto la supervisione e autorizzazione del docente. Costituiscono eccezione i casi di comprovata necessità (situazioni di handicap, certificazione DSA) per i quali è possibile l'utilizzo a scuola del PC personale dell'alunno;
- Si invita il personale scolastico e gli alunni ad avere cura di eventuali dispositivi, compresi quelli personali (es. cellulari, palmari, chiavette, dispositivi di archiviazione o altri documenti), evitando di lasciarli incustoditi e a disposizione di estranei (es. al termine dell'orario lavorativo, durante le pause di lavoro, durante riunioni lontane dalla propria postazione, durante intervalli e cambi di ora, ecc.).

6.2 GESTIONE DOCUMENTALE

Il personale scolastico autorizzato è invitato a:

- Custodire in apposito armadio dotato di serratura i seguenti documenti: registro delle attività di cui si è referenti (es. registro relativo alle attività di teatro, registro IEFP, registro relativo all'alternanza scuola-lavoro, ecc.);
- Consegnare alla segreteria per l'inserimento all'interno dei fascicoli personali ciò che segue:
    1. certificati medici esibiti dagli alunni a giustificazione delle assenze;
    2. qualunque altro documento contenente dati personali o sensibili come certificati di malattia, certificati di pronto soccorso e tutta la documentazione inerente allo stato di salute relativo a un interessato;
- Verificare la corretta funzionalità dei meccanismi di chiusura dell'armadietto personale, segnalando tempestivamente al responsabile di sede eventuali anomalie;
- Riporre la documentazione in modo ordinato e negli appositi contenitori (non trasparenti se si tratta di dati sensibili), chiudendo a chiave classificatori e armadi dove sono custoditi;
- Tutte le comunicazioni indirizzate agli uffici, ad altro personale della scuola e al dirigente scolastico debbono essere consegnate (soprattutto se si tratta di dati sensibili) in busta chiusa al responsabile di sede o al protocollo della sede centrale. Non è consentito l'utilizzo del fax, della posta elettronica e dei collegamenti alla rete internet per il trattamento dei dati sensibili (es. invio tramite mail di certificati di medici);
- Per ogni fascicolo personale degli alunni/personale scolastico le persone autorizzate al trattamento procederanno come segue:
    1. esame di tutti i documenti contenuti nel fascicolo;
    2. catalogare i documenti esaminati, con la distinzione dei documenti contenenti dati personali da quelli contenenti dati sensibili e giudiziari;
    3. i dati sensibili e giudiziari vanno collocati in un sottofascicolo chiuso in tutti e quattro i lati;
    4. tutti i classificatori devono essere dotati di apposite chiavi opportunatamente custodite dalle persone autorizzate (es. collaboratori scolastici);

In particolare per i collaboratori scolastici si raccomanda di:

- Procedere alla chiusura dell'edificio scolastico accertandosi che tutte le misure di protezione dei locali siano state attivate;
- Non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali o sensibili ma accertarsi che vengano sempre distrutte e/o rese anonime;
- Non consentire che estranei possano accedere ai documenti dell'ufficio o leggere documenti contenenti dati personali o sensibili;
- Procedere alla chiusura dei locali non utilizzati in caso di assenza del personale scolastico;

6.3 GESTIONE PASSWORD E CODICI DI ACCESSO

Le seguenti regole per la gestione delle password si applicano a tutti i servizi informatici, gestionali ed applicativi (compresi quelli web), alle postazioni di lavoro, alla rete wi-fi (ove presenti), al servizio di posta elettronica e a tutte le applicazioni e risorse informatiche (es. registro elettronico) presenti all'interno dell'istituto che prevedono un sistema di autenticazione per l'accesso.

- Il personale scolastico e gli alunni non devono comunicare e/o condividere la propria password personali con nessun'altra persona all'interno dell'organizzazione, (colleghi, alunni, personale scolastico, ecc.) e all'esterno (amici, conoscenti, ecc.);
- Nei casi in cui l'utente perda il ruolo, la mansione e le qualità che gli consentono di utilizzare le credenziali per accedere ai vari servizi dell'istituto scolastico le stesse credenziali devono essere disattivate (es. in caso di cessazione del rapporto di lavoro, trasferimento, demansionamento, licenziamento, sostituzione, ecc.);
- Evitare di memorizzare password e credenziali di accesso su fogli di carta, documenti cartacei e file conservati all'interno della postazione di lavoro (es. non trascrivere la propria password su post it o fogli presso la propria postazione, non deve essere memorizzata in funzioni di log-in automatico, in un tasto funzionale o nel browser utilizzato per la navigazione internet);
- Gli utenti nella scelta della password devono evitare combinazioni facili da identificare (evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili). Devono scegliere password univoche e originali, che abbiano un senso solo per l'utente che le sceglie, evitando di usare la stessa password per altre utenze.

La password deve essere ragionevolmente complessa e difficile da individuare e/o ricavare. Nei limiti tecnici consentiti dai sistemi, la password (es. la password d'accesso relative al computer, alla rete, a programmi e software specifici, al salvaschermo):

1. deve essere di lunghezza non inferiore ad 8 caratteri;
2. deve essere obbligatoriamente cambiata al primo utilizzo e successivamente almeno una volta ogni 3 mesi, o nei casi in cui sia compromessa;
3. deve contenere, ove possibile, almeno 3 caratteri tra numeri, caratteri alfabetici in maiuscolo e minuscolo, e caratteri speciali.

6.4 GESTIONE POSTA ELETTRONICA E MAIL

- Gli utenti (es. il personale scolastico) devono utilizzare la propria mail (es. @istruzione.it) per soli fini professionali tenendola separata dalla e-mail privata;
- Nel caso in cui qualcuno appartenente alla comunità scolastica (alunno, docente, personale) riceva e-mail da considerare particolarmente preoccupanti (es. mail con contenuti pedo pornografici) dovrà mettersi in contatto con il personale scolastico e/o, a seconda della gravità, direttamente con gli organi di Polizia Postale;
- L'utente non dovrà utilizzare la posta elettronica per il trasferimento di dati sensibili relativo al personale o relativo agli alunni. Se non esiste una soluzione alternativa al trasferimento sicuro dei file, si dovrà provvedere in modi diversi (es. riferire direttamente di persona, consegna cartacea della documentazione);
- Ogni utente che utlizza la posta elettronica dovrà prestare massima attenzione a rispondere ad e-mail sospette e/o a cliccare sui link durante la navigazione web (o su link presenti all'interno delle mail) al fine di contrastare possibili frodi informatiche (come il phishing, lo spear phishing, il furto d'identità, ecc.);
- Il personale scolastico potrà mettersi in comunicazione con alunni e genitori (e viceversa) solo per ragioni e fini chiaramente istituzionali e professionali utilizzando gli appositi canali ufficiali;
- Per un corretto utilizzo della posta elettronica l'utente è invitato a:
  1. non aprire documenti di cui non sia certa la provenienza;
  2. controllare accuratamente l'indirizzo dei destinatari prima di inviare dati personali.

6.5 GESTIONE BACK UP E CLOUD COMPUTING

- Gli utenti sono invitati a non condividere e/o memorizzare dati personali relativi alla propria sfera privata (foto della propria famiglia e/o amici, dei luoghi di abitazione, amici, ecc) all'interno dello spazio online e/o supporti di archiviazione appartenenti all'istituto scolastico;
- Il personale scolastico è invitato a non condividere e/o memorizzare dati personali relativi alla propria attività istituzionale (es. dati personali e sensibili relativi agli studenti) su servizi di hosting pubblici (es. Google Drive, Dropbox, ecc) salvo specifiche e chiare autorizzazioni da parte del Dirigente Scolastico;
- In casi di supporti (es. usb, dispositivi di archiviazione mobili, ecc.) contenenti dati sensibili devono essere chiaramente identificati e non devono mai essere lasciati incustoditi.

6.6 SOCIAL NETWORK E NAVIGAZIONE INTERNET

Il personale scolastico (es. insegnanti, esperti, educatori, collaboratori, ecc.):

- Non dovrà intraprendere attività online (es. attraverso l'utilizzo di social, chat, forum, blog, ecc.) che possa compromettere la propria reputazione, le proprie responsabilità professionali e che possa portare discredito all'Istituto scolastico con le sue opinioni personali. Si raccomanda quindi di:

1. Evitare di scaricare/inviare materiali che possano essere considerati offensivi o di natura estremista;
2. Assicurare che tutti gli spazi social e di condivisione utilizzati come privato cittadino siano nettamente distinti e non possano essere confusi con il proprio ruolo professionale (es. non fare riferimento a studenti/alunni, genitori/tutori o personale scolastico, non entrare in discussioni online su questioni personali relative agli stessi membri della comunità scolastica, non attribuire opinioni personali alla scuola o alla sua dirigenza o alle autorità locali; ecc.);

- Dovrà utilizzare i sistemi dedicati, ufficiali e istituzionali della scuola per l'effettuazione di eventuali comunicazioni nei confronti di studenti e famiglie (es. tramite utilizzo di apposita mail istituzionale);
- Non organizzerà a titolo personale spazi social network, seppur riguardanti progetti didattici o comunque legati all'apprendimento scolastico, da usare in collaborazione con gli studenti senza previa autorizzazione della Dirigenza;
- E' invitato a prestare attenzione a eventuali diritti d'autore (royalty) prima di pubblicare o distribuire qualsiasi manufatto intellettuale tra cui immagini, musica, video, registrazioni vocali;
- E' invitato (insieme agli alunni e a qualsiasi altro utente) nei casi in cui si utilizzi internet, a non aprire, scaricare, installare o utilizzare file/applicazioni/software (es. videogiochi) sospetti e/o di dubbia provenienza (si raccomanda l'utilizzo del protocollo HTTPS) o il cui utilizzo non sia stato preventivamente approvato e autorizzato dalla Dirigenza;
- E' invitato a prestare massima attenzione in caso di comportamenti anomali e fastidiosi su social network (es. Facebook, Twitter, Instagram, ecc.) su sistemi di messaggistica istantanea, salvaguardando, per quanto possibile, che gli studenti, in caso di utilizzo di smathphone o altra apparecchiatura elettronica all'interno dell'istituto scolastico, non diffondano immagini e dati personali senza previa consenso dell'interessato (proprietario del dato).

- E' invitato a mantenere la massima riservatezza riguardo al segreto d'ufficio e professionale (es. riguardo a dati eventualmente contenuti nei temi degli alunni specialmente se riguardano argomenti delicati e strettamente relativi alla sfera privata, riguardo alle condizioni di salute di colleghi e studenti, ecc.)

Le famiglie e gli alunni:

- Sono resi consapevoli che l'istituto scolastico prenderà precauzioni ragionevoli per mettere in sicurezza i propri utenti evitando che gli studenti accedano a materiali inappropriati;
- Sono invitati a sostenere e collaborare con l'istituto scolastico promuovendo l'uso sicuro di Internet e delle tecnologie digitali a casa, informando la scuola in caso di preoccupazioni al riguardo;
- Nel caso in cui gli stessi alunni vedano o sentano qualcosa che possa turbare la propria privacy (ad es. la ricezione di un messaggio che possa farli sentire a disagio) sono invitati a parlarne con un adulto di fiducia (genitori o nel caso i propri docenti).

6.7 GESTIONE STRUMENTAZIONE PERSONALE: USO DEI CELLULARI E DISPOSITIVI MOBILI

REGOLE GENERALI

- Il personale, esperti di progetto, gli studenti, i genitori e/o i visitatori che portano all'interno dell'Istituto device di loro proprietà, sono responsabili del proprio dispositivo e lo portano nell'Istituto a proprio rischio. Si puntualizza che se il device viene smarrito, si rompe, viene danneggiato, vengono persi dei dati ecc. la scuola non deve essere considerata responsabile della sicurezza di tali dispositivi/dati né deve farsi carico di eventuali risarcimenti;
- L'istituzione scolastica si riserva il diritto di reperire contenuti presenti all'interno di qualsiasi dispositivo presente nei locali della scuola in cui vi sia il ragionevole sospetto che possa contenere materiale illegale o indesiderabile (es. la pornografia, la violenza o il bullismo, registrazioni di qualsiasi genere vietate, ecc…). L'ispezione potrà avvenire in presenza di pubblico ufficiale;
- L'utilizzo del cellulare, di apparecchi per la registrazione di suoni e immagini è in genere consentito, ma esclusivamente per fini didattici (recite, video lezioni, attività progettuali, ecc.), nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte, in particolare della loro immagine e dignità;
- Si ricorda che prima di ogni utilizzo o eventuale diffusione, anche su Internet, diverso dalle finalità didattiche e istituzionali, è necessario informare adeguatamente le persone coinvolte nella registrazione (professori, studenti, ecc…) e ottenere il loro esplicito consenso; in ogni caso deve essere sempre garantito il diritto degli studenti con diagnosi DSA (disturbi specifici dell'apprendimento) o altre specifiche patologie l'utilizzo di tutti gli strumenti compensativi di volta in volta previsti nei piani didattici personalizzati che li riguardano;
- Non violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici. Le immagini in questi casi sono raccolte a fini personali e destinati ad un ambito familiare o amicale. Nel caso si intendesse pubblicarle e diffonderle in rete, anche sui social network, è necessario ottenere di regola il consenso delle persone presenti nei video o nelle foto.

PER GLI STUDENTI E FAMIGLIE

Caso 1. Utilizzo del telefono cellulare/tablet/altri dispositivi mobili personali ad uso assimilabile al privato per chiamate, sms, messaggistica in genere, ecc.

- Si ribadisce che durante l'orario delle lezioni (es. durante gli esami, verifiche, prove nazionali) l'uso di device personali non è consentito (es. per ricevere/effettuare chiamate, navigazione su internet, SMS o altro tipo di messaggistica, gioco, ecc.);
- Gli alunni sono tenuti a fare buon uso dei propri telefoni/device (es. riporli in un luogo non visibile durante l'intera permanenza a scuola);
- Per quanto riguarda uscite visite guidate e viaggi di istruzione l'uso può essere consentito, se autorizzato dal docente, al di fuori dei momenti dedicati a visite guidate e attività legate all'aspetto didattico dell'uscita;
- La comunicazione con le famiglie, per qualsiasi urgenza, è sempre garantita attraverso il telefono della scuola (I docenti possono però consentire l'uso del cellulare, in caso di particolari situazioni non facilmente risolvibili in altro modo, ad es. in casi di particolare emergenza e grave pericolo per le persone;
- Le famiglie degli studenti sono invitate a collaborare strettamente con l'Istituzione scolastica nello spirito della corresponsabilità educativa (es. evitando di inviare messaggi o effettuare chiamate ai telefoni dei propri figli durante l'orario scolastico o visite di istruzione).

Caso 2. Utilizzo delle funzioni tipiche degli smartphone, tablet, notebook e altri dispositivi mobili (foto, video, scrittura collaborativa e condivisione di documenti, ecc.), per le attività didattiche a scopi professionali.

- In questo caso l'uso di smartphone, tablet e altri dispositivi mobili personali , è consentito. I dispositivi mobili personali verranno utilizzati unicamente durante le lezioni solo come parte di un'attività curriculare e secondo le modalità prescritte dall'insegnante e con esclusiva finalità didattica;
- Si ribadisce che immagini, video, registrazioni vocali (e relativa diffusione) possono essere effettuate per finalità didattiche e istituzionali previo consenso della persona o persone in questione a cui si riferiscono (nei casi di minori di 14 anni il consenso va richiesto ai tutori legali/genitori);
- Si ricorda che la diffusione di filmati e foto che ledono la riservatezza e la dignità di sé e di altre persone (es. eventuali riprese audio/video o fotografiche effettuate all'interno degli ambienti scolastici e successivamente diffuse con l'intento di ridicolizzare compagni o insegnanti o addirittura allo scopo di intraprendere azioni denigratorie, intimidatorie, vessatorie) può far incorrere lo studente in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati. Anche in questo caso si richiedono grande sintonia e collaborazione tra scuola e famiglia, in modo da favorire lo sviluppo della necessaria consapevolezza e maturità circa l'utilizzo degli strumenti ai quali gli studenti abbiano accesso.

PER IL PERSONALE SCOLASTICO (ES. DOCENTI, EDUCATORI, ESPERTI DI PROGETTO)

- L'uso di smartphone, tablet e altri dispositivi mobili è consentito con esclusiva finalità professionale e solo in caso di particolari necessità (es. evacuazione dell'Istituto, emergenze);
- L'uso del cellulare/tablet non è consentito, salvo autorizzazione della Dirigenza, per ricevere/effettuare chiamate personali, SMS o altro tipo di messaggistica durante l'orario di lavoro.

7 GESTIONE VIOLAZIONI/INFRAZIONI E CODICE SANZIONATORIO

In conclusione all'interno dell'Istituzione Scolastica si richiede la comprensione e il rispetto dei contenuti indicati all'interno del presente Regolamento Privacy da parte di tutti i soggetti coinvolti per il trattamento dei dati personali all'interno della comunità scolastica.
Qualsiasi sospetto, rischio, violazione, uso improprio di device e supporti sui quali "viaggi" il dato personale, va segnalato in giornata al Dirigente Scolastico. Il personale, genitori e gli stessi alunni sono invitati a supportare la sicurezza a scuola segnalando qualsiasi comportamento inappropriato di alunni, docenti, dipendenti e membri della comunità scolastica. Questi ultimi verranno segnalati al Dirigente, e nel caso, direttamente alle autorità competenti. Al personale, agli studenti e agli altri componenti della comunità scolastica sono date informazioni sulle infrazioni previste e le eventuali sanzioni. Le sanzioni riferite soprattutto agli alunni avranno come carattere preferenziale quello educativo/riabilitativo e in ogni caso verrà coinvolta la componente genitori, in qualità di primi educatori.
Si informano gli studenti e tutti i membri della comunità scolastica che infrangono quanto citato come "violazioni-infrazioni" (elencate a titolo esemplificativo e non esaustivo) all'interno della seguente tabella riassuntiva che la decisione finale sul livello di sanzione applicata è affidata agli organi competenti previsti a seconda dei casi. Laddove se ne valuti la necessità si farà riferimento anche alle norme generali di comportamento già in essere e sempre valide con relative procedure disciplinari.

STUDENTI	
VIOLAZIONI - INFRAZIONI	**ORGANO COMPETENTE E AZIONI/SANZIONI POSSIBILI**
• L'alunno usa in modo non autorizzato e inappropriato (es. utilizzando lo smartphone/device scolastico e/o privato durante la lezione o una verifica scritta, durante gli esami, per copiare e/o reperire informazioni; naviga su siti internet non appropriati durante la lezione, usa software non autorizzati, ecc.)	• Si fa spegnere il device, lo si deposita in segreteria e lo si restituisce al termine delle lezioni (eventualmente ai genitori contestualmente convocati); • Nota disciplinare sul registro di classe (può essere previsto il ritiro della verifica e valutazione gravemente insufficiente della stessa);
• L'alunno continua (nonostante precedente ammonimento) ad usare in modo non autorizzato e inappropriato (es. utilizzando lo smartphone/device scolastico e/o privato durante la lezione o una verifica scritta, durante gli esami, per copiare e/o reperire informazioni; naviga su siti internet non appropriati durante la lezione, usa software non autorizzati, ecc.)	• Si fa spegnere il device, lo si deposita in segreteria e lo si restituisce al termine delle lezioni (eventualmente ai genitori contestualmente convocati); • Nota disciplinare sul registro di classe (può essere previsto il ritiro della verifica e valutazione gravemente insufficiente della stessa, sospensione dei diritti di accesso alla rete e agli ambienti social di istituto per un periodo congruo)
• L'alunno deliberatamente diffonde/pubblica/condivide/modifica/cancella in modo non autorizzato e inappropriato immagini/video/audio su social network o piattaforma online autorizzata dall'istituto scolastico; • L'alunno spedisce mail o messaggi istantanei che possono essere considerati molestia, contenenti caratteri di bullismo;	• Si fa spegnere il device, lo si deposita in segreteria e lo si restituisce al termine delle lezioni (eventualmente ai genitori contestualmente convocati); • Si riferisce tempestivamente al coordinatore di classe e al dirigente scolastico; • Nota disciplinare sul registro di classe; • Si prendono adeguati provvedimenti disciplinari in accordo con il consiglio di classe: es. abbassamento voto in condotta sospensione dalle uscite didattiche sospensione dalle lezioni • Sospensione dei diritti di accesso alla rete e agli ambienti social di istituto per un periodo congruo; • Si prendono contatti con fornitori di servizi coinvolti (ove presenti) per rimuovere il materiale incriminato per garantire che non vi sia alcun rischio per i diritti degli interessati;
• L'alunno continua deliberatamente a diffondere/pubblicare/condividere/modificare/cancellare in modo non autorizzato e inappropriato immagini/video/audio su un qualsiasi social network o piattaforma online autorizzata dall'istituto scolastico; • L'alunno deliberatamente crea spazi per l'accesso, la diffusione e/o lo scaricamento di qualsiasi materiale offensivo ritenuto , osceno, diffamatorio, razzista, omofobico o violento;	• Si fa spegnere il device, lo si deposita in segreteria e lo si restituisce al termine delle lezioni (eventualmente ai genitori contestualmente convocati); • Comunicazione immediata Dirigente, al coordinatore di classe, eventualmente al Consiglio di istituto convocando i genitori; • Si prendono adeguati provvedimenti disciplinari in accordo con il consiglio di classe: es. abbassamento voto in condotta sospensione dalle uscite didattiche sospensione dalle lezioni

• L'alunno trasmette materiale che viola le norme del diritto d'autore (copyright) o i diritti di privacy;	• Sospensione dei diritti di accesso alla rete e agli ambienti social di istituto per un periodo congruo (indeterminato) • Si prendono contatti con fornitori di servizi coinvolti (ove presenti) per rimuovere il materiale incriminato per garantire che non vi sia alcun rischio per i diritti degli interessati; • Si comunica alla Polizia Postale o agli enti preposti alla denuncia di abusi, cyberbullismo o altre attività sospette;
MEMBRI MAGGIORENNI DELLA COMUNITA' SCOLASTICA (personale scolastico, staff, educatori, docenti, personale amministrativo e collaboratori, genitori, studenti ed equiparati)	
INFRAZIONI – CATTIVA CONDOTTA	**ORGANO COMPETENTE E AZIONI/SANZIONI POSSIBILI**
• Uso di Internet e dei device privati per attività personali e non in relazione con il proprio profilo e/o sviluppo professionale (es. mail personali, navigazione su siti inadeguati, ecc.); • Uso di archivi conservazione dati sensibili degli alunni o dei membri della comunità scolastica (es. chiavette USB) senza considerare la possibilità di accesso agli stessi da parte di terzi non autorizzati o senza considerare l'adeguatezza di qualsiasi file memorizzato; • Qualsiasi comportamento che comprometta la professionalità del personale della comunità scolastica; • Utilizzo illecito o condivisione di password; • Violazione del copyright o licenza (per esempio l'installazione di software senza licenza in rete)	• Comunicazione al dirigente scolastico; • Ammonizione informale a voce; • Ammonizione formale scritta;
• Abuso grave o danneggiamento intenzionale di qualsiasi hardware computer o software della scuola; • Qualsiasi tentativo deliberato di violare le norme sulla protezione dei dati o di sicurezza informatica; • La creazione deliberata, l'accesso, il download e la diffusione di qualsiasi materiale ritenuto offensivo osceno, diffamatorio, razzista, omofobico o violento.	• Immediata denuncia al Dirigente scolastico o agli organi competenti; • Si prendono contatti con fornitori di servizi coinvolti (ove presenti) per rimuovere il materiale incriminato per garantire che non vi sia alcun rischio per i diritti degli interessati; • Comunicazione alla Polizia Postale o agli enti preposti alla denuncia di abusi, o altre attività sospette e illecite.
Nel caso in cui un membro della comunità scolastica commetta un atto di colpa eccezionalmente grave (es. in caso di ritrovamento di immagini con abuso di minori), lo stesso verrà immediatamente sospeso, soprattutto se vi è un reale pericolo per un minore. Tuttavia prima che venga presa un'azione disciplinare rispetto a qualsiasi reato, si procederà all'effettuazione di un'opportuna inchiesta. Al soggetto, verrà chiesto di spiegare le sue azioni e queste saranno prese in considerazione prima di intraprendere qualsiasi azione disciplinare. Per poter indagare, la scuola potrà avvalersi di agenzie di supporto esterne (per esempio un servizio di supporto tecnico per indagare circa attrezzature e dati eventualmente presenti come possibili prove), delle autorità locali e territoriali di riferimento.	

8 NOTE CONCLUSIVE

In conclusione si invitano tutti i membri della comunità scolastica (personale docente, collaboratori, famiglie e alunni, ecc.) a collaborare strettamente con l'Istituzione scolastica nello spirito della corresponsabilità educativa e della salvaguardia della protezione dei dati personali. Chiunque può segnalare gratuitamente tramite i canali istituzionali della scuola, qualsiasi attività on-line, trattamento non autorizzato e/o trattamento illecito di dati personali.

IL DIRIGENTE SCOLASTICO
Prof.ssa Roberta Fantinato
Firma autografa sostituita a mezzo stampa ai sensi e per gli effetti dell'art. 3, c. 2, D. lgs. N. 39/93

APPROVATO CON DELIBERA N. 47 dal CONSIGLIO DI ISTITUTO in data 20 dicembre 2018.