Documento di ePolicy
I.C. SETTIMO S. PIETRO

VIA CARDUCCI 1 - 09040 - SETTIMO SAN PIETRO
Cagliari (CA) - Sardegna
Data di approvazione: 07/05/2026 - 10:52

Cap 1 - Lo scopo della ePolicy

1.1 Scopo della ePolicy

Capitolo 1 - Presentazione dell'ePolicy

1. Scopo dell'ePolicy
2. Ruoli e responsabilità nell'implementazione dell'ePolicy
3. Integrazione dell'ePolicy con regolamenti e normativa generale esistenti
4. Condivisione e comunicazione dell'ePolicy all'intera comunità educante
5. I piani di Azione dell'ePolicy

Capitolo 2 - Sensibilizzazione e prevenzione

1. Sensibilizzazione e prevenzione
2. Il Curricolo Digitale
3. IL KIT DIDATTICO

Capitolo 3 - Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola

1. Protezione dei dati personali e GDPR
2. Accesso ad Internet
3. Strumenti di comunicazione online (PUA)
4. Strumentazione personale (BYOD)

Capitolo 4 - Segnalazione e gestione dei casi

1. Cosa segnalare
2. Come segnalare: quali strumenti e a chi
3. Gli attori sul territorio per intervenire
4. Allegati con le procedure

1.1 Scopo dell'ePolicy

(Questo paragrafo illustra lo scopo e gli obiettivi di questo documento programmatico per la cittadinanza digitale)

L' E-Policy ha come obiettivo principale quello di promuovere le competenze digitali per un uso delle tecnologie digitali positivo, critico e consapevole, da parte degli studenti e delle studentesse guidati dagli adulti coinvolti nel processo didattico-educativo.

La competenza digitale è una competenza chiave del cittadino europeo come indicato dal Consiglio Europeo

(Raccomandazione del 2018) che permette ad ogni cittadino di esercitare i propri diritti all'interno degli ambienti digitali (ONU - Commento Generale 25: I diritti dei minori negli ambienti digitali).

L'ePolicy è un documento programmatico che permette di lavorare su quattro obiettivi:

1. Il piano di azioni triennale per promuovere nell'intera comunità scolastica l'uso sicuro responsabile e positivo della rete;
2. le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
3. le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
4. le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

L'Istituto Comprensivo di Settimo San Pietro (Codice Meccanografico: CAIC84700T) ha aggiornato il presente documento di ePolicy per il triennio 2025-2028, in coerenza con le priorità strategiche definite nel Piano Triennale dell'Offerta Formativa (PTOF). L'Istituto Comprensivo di Settimo San Pietro ha effettuato sulla piattaforma Generazioni Connesse un primo caricamento dell' E-Policy in data 11/06/2020 e oggi, ritenendo utile aggiornarlo nelle sue specificità, lo adotta come strumento operativo al servizio di tutta la comunità educante al fine di assicurare un approccio consapevole, critico, efficace nei confronti della tecnologia e sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso improprio della rete.

L'utilizzo di Internet ha rivoluzionato in modo radicale il nostro modo di vivere tantoché nella nuova generazione dei cosiddetti "Nativi digitali" si riscontra un uso della rete sempre più precoce attraverso una gamma via via più ricca di dispositivi facilmente alla loro portata. Tutto ciò da un lato risulta positivo in quanto la rete offre, soprattutto per i bambini e per gli adolescenti, opportunità di accrescimento del sapere, di incremento delle capacità comunicative, di sviluppo delle competenze e di miglioramento delle prospettive di lavoro, ma d'altra parte può esporre a situazioni insidiose di vulnerabilità che richiedono interventi specifici. L'ePolicy del nostro Istituto ha lo scopo di adottare
una linea strategica affinché tutta la comunità scolastica possa muoversi con sicurezza e competenza negli ambienti digitali tramite:

-l'individuazione di norme comportamentali inerenti l'utilizzo delle TIC;
-la promozione dell'uso positivo delle TIC nella didattica;
-l'adozione di misure per la prevenzione del fenomeno del cyberbullismo con strumenti di tutela in caso di comportamenti vessatori e di emarginazione tramite un uso distorto e violento della rete;
-la sensibilizzazione degli studenti ad un uso corretto delle tecnologie digitali.

Pertanto l'I.C. Settimo San Pietro riconosce le Tecnologie dell'Informazione e della Comunicazione (TIC) come motori essenziali per l'innovazione didattica e l'inclusione sociale e coerentemente con il Piano Triennale dell'Offerta Formativa (PTOF) 2025-2028, l'ePolicy non è intesa solo come un regolamento, ma come un documento programmatico volto a:

● Promuovere la Cittadinanza Digitale: dotare gli studenti delle competenze chiaveeuropee per un uso consapevole, critico e creativo degli strumenti digitali.
● Sostenere l'Inclusione: utilizzare le tecnologie come mediatori facilitatori per gli alunni con Bisogni Educativi Speciali (BES) e per supportare l'integrazione di gruppi vulnerabili del territorio.
● Valorizzare il PNRR (Missione 4): integrare i nuovi laboratori STEM (DM 65/2023) e i percorsi di formazione sulla transizione digitale (DM 66/2023) in un quadro di sicurezza
e responsabilità condivisa.

Obiettivi Strategici

In linea con l'analisi del contesto territoriale e le priorità di miglioramento dell'Istituto, l'ePolicy mira a raggiungere i seguenti traguardi triennali:

Obiettivo 1 Benessere Digitale

Descrizione Operativa: Prevenire e contrastare episodi di cyberbullismo e disagio online attraverso la rete territoriale (PLUS 21).

Obiettivo 2 Innovazione Didattica

Descrizione operativa: Promuovere l'uso positivo dei social e del digital storytelling per la valorizzazione del patrimonio locale (Progetto Arca del Tempo).

Obiettivo 3 Corresponsabilità

Descrizione operativa: Rafforzare l'alleanza educativa con le famiglie per una gestione condivisa della vita digitale degli studenti.

Destinatari
L'ePolicy si rivolge all'intera comunità educante dell'I.C. Settimo San Pietro: studenti, docenti, personale ATA e genitori.

Il documento è parte integrante del Patto di Corresponsabilità e viene aggiornato periodicamente per rispondere alle evoluzioni tecnologiche e alle specifiche esigenze emerse dal monitoraggio dei bisogni del territorio.

Infine l'ePolicy si integra con le nuove linee di indirizzo del Piano Nazionale di Ripresa e Resilienza (PNRR) e le recenti disposizioni ministeriali:

- Transizione Digitale (DM 66/2023): l'istituto promuove la formazione alla transizione digitale per tutto il personale scolastico nell'ambito della Missione 4 del PNRR .
- Competenze STEM e Linguistiche (DM 65/2023): Potenziamento dei linguaggi e delle competenze digitali per gli studenti.
- Protocolli di Rete: Collaborazione con il PLUS 21 per l'erogazione di interventi specializzati quali la prevenzione del bullismo e del cyberbullismo, la consulenza legale e la mediazione familiare.

1.2 - ePolicy: ruoli e responsabilità nell'implementazione dell'ePolicy

- (In questo paragrafo vengono dettagliati ruoli e responsabilità nell'implementazione del documento all'interno dei contesti scolastici ivi inclusi rappresentanti genitori e studenti per secondaria II grado).

Affinché l'ePolicy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, s'impegni nell'attuazione e promozione di essa.

È opportuno che nel documento vengano definiti con chiarezza ruoli, compiti e responsabilità di ciascuna delle figure all'interno dell'Istituto.

In questo paragrafo dell'ePolicy è importante specificare le figure professionali che, a vario titolo, si occupano di gestione e programmazione delle attività formative, didattiche ed educative dell'Istituto e tutte quelle figure appartenenti alla comunità educante.

IL DIRIGENTE SCOLASTICO

Il ruolo del Dirigente Scolastico nel promuovere l'uso consentito delle tecnologie digitali e di internet include i seguenti compiti:

- promuovere la cultura della sicurezza online e garantirla a tutti i membri della comunità scolastica, in linea con il quadro normativo di riferimento, le indicazioni del MIM, delle sue agenzie e attraverso il documento di ePolicy;
- promuovere la cultura della sicurezza online – anche attraverso il documento di ePolicy - integrandola ed inserendola nelle misure di sicurezza più generali dell'intero Istituto;
- ha la responsabilità di fornire sistemi per un uso sicuro delle TIC, internet, i suoi strumenti ed ambienti e deve garantire alla popolazione scolastica la sicurezza di navigazione tramite internet utilizzando adeguati sistemi informatici e filtri;
- ha la responsabilità della gestione dei dati e della sicurezza delle informazioni e garantisce che l'Istituto segue le pratiche migliori possibili nella gestione dei dati stessi;
- deve tutelare la scuola e garantire agli utenti la sicurezza di navigazione utilizzando adeguati sistemi informatici e servizi di filtri Internet;
- ha il compito di garantire a tutto il personale una formazione adeguata sulla sicurezza online per essere tutelato nell'esercizio del proprio ruolo educativo e non;
- deve essere a conoscenza delle procedure da seguire in caso di un grave incidente di sicurezza online;
- deve garantire adeguate valutazioni di rischio nell'usare strumenti e TIC, effettuate in modo che comunque quanto programmato possa soddisfare le istanze educative e didattiche dichiarate nel PTOF di Istituto;
- deve garantire l'esistenza di un sistema che assicuri il monitoraggio e il controllo interno della sicurezza online in collaborazione con le figure di sistema;
- deve essere a conoscenza ed attuare le procedure necessarie in caso di grave incidente di sicurezza online.

L'ANIMATORE DIGITALE E IL TEAM PER L'INNOVAZIONE DIGITALE

L'animatore digitale e il Team per l'Innovazione digitale sono co-responsabili, con il referente ePolicy, dell'attuazione dei piani di azione in particolare in riferimento alla formazione dei docenti. Sono inoltre responsabili del controllo all'accesso da parte degli studenti delle Tic

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

Il referente cyberbullismo è co-responsabile, con il team ePolicy, dell'attuazione dei piani di azione e coordina le iniziative di prevenzione e contrasto del cyberbullismo.

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

In coerenza con le Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo del Ministero

dell'Istruzione (D.M. n. 18 del 13/1/2021, agg. 2021 – nota prot. 482 del 18-02-2021), il Team ha le funzioni di coadiuvare il Dirigente Scolastico, coordinatore del Team nella scuola, nella definizione degli interventi di prevenzione e nella gestione dei casi di bullismo e cyberbullismo che si possono presentare. Promuove inoltre la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale e comunica ad alunni, famiglie e tutto il personale scolastico dell'esistenza del team, a cui poter fare riferimento per segnalazioni o richieste di informazioni sul tema.

Il Team ha il compito di:

- coadiuvare il Dirigente scolastico, coordinatore del Team, nella definizione degli interventi di prevenzione del bullismo (per questa funzione partecipano anche il presidente del Consiglio d'Istituto e i Rappresentanti degli studenti).
- Intervenire (come gruppo ristretto, composto da Dirigente e referente o referenti per il bullismo e il cyberbullismo, psicologo o pedagogista, se presente) nelle situazioni acute di bullismo.
- Promuovere la redazione e l'applicazione della ePolicy e monitorare le segnalazioni.

I/LE DOCENTI

I/le docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Possono, innanzitutto, integrare la propria disciplina con approfondimenti, promuovendo l'uso delle tecnologie digitali nella didattica. I docenti devono accompagnare e supportare gli/le studenti nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete. Inoltre, educano gli studenti alla prudenza, a non fornire dati ed informazioni personali, ad abbandonare un sito dai contenuti che possono turbare o spaventare e a non incontrare persone conosciute in Rete senza averne prima parlato con i genitori. Informano gli alunni sui rischi presenti in Rete, senza demonizzarla, ma sollecitandone un uso consapevole, in modo che Internet possa rimanere per bambini/e e ragazzi/e una fonte di divertimento e uno strumento di apprendimento.

I/le docenti osservano altresì regolarmente i comportamenti a rischio (sia dei potenziali bulli, sia delle potenziali vittime) e hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che veda coinvolti studenti e studentesse dandone tempestiva comunicazione al Dirigente Scolastico, al Referente per il Cyberbullismo e Bullismo e al Consiglio di Classe per definire strategie di intervento condivise.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Responsabile della protezione dei dati (RPD o DPO) conosce l'ePolicy di Istituto, fornisce la propria consulenza in merito agli obblighi derivanti dal GDPR e sorveglia sull'esatta osservanza della normativa in materia di tutela dei dati personali ed è co-responsabile delle azioni di informazione e formazione nell'Istituto sulla protezione dei dati personali

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

Il personale ATA, all'interno dei singoli regolamenti d'Istituto, è coinvolto nelle pratiche di prevenzione – ivi incluso il processo di definizione e implementazione dell'ePolicy di Istituto - ed è tenuto alla segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo.

GLI STUDENTI E LE STUDENTESSE

Gli studenti e le studentesse devono, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti. Con il supporto della scuola dovrebbero imparare a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le. Affinché questo accada devono partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education.

I rappresentanti degli/delle studenti sono informati del documento di ePolicy e invitati a costruire i piani di azione, a partire dal secondo anno della secondaria di II grado,

I GENITORI/ADULTI DI RIFERIMENTO

I Genitori, in continuità con l'Istituto scolastico, sono attori partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile degli strumenti personali (pc, smartphone, etc). Come parte della comunità educante sono tenuti a relazionarsi in modo costruttivo con i/le docenti sulle linee educative che riguardano le TIC e la Rete e – ivi incluso il documento di ePolicy - comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet.

È estremamente importante che accettino e condividano quanto scritto nell'ePolicy d'Istituto e nel patto di corresponsabilità in un'ottica di collaborazione reciproca. Si promuove il coinvolgimento dei rappresentanti di genitori/adulti di riferimento all'interno del percorso di definizione e implementazione dell'ePolicy.

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

Enti esterni pubblici e privati, il mondo dell'associazionismo dovranno conformarsi alla politica della scuola riguardo all'uso consapevole delle TIC e della rete per la realizzazione di iniziative nelle scuole, finalizzate a promuovere un uso positivo e consapevole delle Tecnologie Digitali da parte dei più giovani, e/o finalizzate a prevenire e contrastare situazioni di rischio online e valutare la rispondenza delle proposte di attività di sensibilizzazione/formazione alle esigenze di qualità contenute nel documento di ePolicy. Dovranno inoltre promuovere comportamenti sicuri durante le attività che si svolgono con gli/le studenti e verificare di aver implementato una serie di misure volte a garantire la tutela dei minori nel caso di insorgenza di problematiche e ad assicurarne la tempestiva individuazione e presa in carico.

Sulla base di quanto enunciato, tutti gli attori coinvolti, nel rispetto ciascuno dei propri si impegneranno nell'attuazione e promozione del documento. In particolare nel nostro isituto:
Il Dirigente Scolastico si impegnerà a garantire la sicurezza, anche online, di tutti i membri della comunità scolastica, attraverso una formazione sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIUR. Tale formazione, valutata e organizzata con la collaborazione del docente referente sulle tematiche del bullismo / cyberbullismo e del team digitale é volta a promuovere la cultura della sicurezza online e sarà estesa, ove possibile, a tutte le figure scolastiche per promuovere un utilizzo positivo e responsabile delle TIC.
L'Animatore digitale supporterà il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale"; potrà, inoltre, qualora, necessario, monitorare e rilevare eventuali episodi o problematiche connesse all'uso delle TIC a scuola.

Il Referente per il bullismo e il cyberbullismo avrà il compito di coordinare e promuovere iniziative specifiche per la

prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, potrà avvalersi della collaborazione, oltre che del team antibullismo, delle Forze di polizia, delle associazioni operanti nel territorio e delle iniziative promosse dai Servizi Sociali e Culturali dell'Amministrazione Comunale.

I Docenti avranno un ruolo centrale nella diffusione delle Tic e nell'utilizzo della rete, integrando l'uso delle tecnologie digitali nella propria didattica e avranno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che veda coinvolti studenti e studentesse.

Il personale Amministrativo, Tecnico e Ausiliario (ATA) sarà coinvolto, a seconda dei propri ambiti di pertinenza anche nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo che magari si evidenziano nei corridoi, nei bagni o in altri ambienti che possono sfuggire all'immediato controllo da parte dei docenti.

Gli Studenti e le Studentesse dovranno, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzare al meglio le tecnologie digitali sotto la guida dei docenti, imparando a tutelare se stessi e gli altri, partecipando attivamente ai progetti ed attività che verranno proposti riguardo l'uso positivo delle TIC e della Rete.

I Genitori, in continuità con l'Istituto scolastico, accettando e condividendo quanto scritto nell'ePolicy dell'Istituto, dovranno essere partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali, relazionandosi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicando con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet.

Agli Enti educativi esterni e le associazioni che dovessero entrare in relazione con la scuola sarà richiesto di prendere visione dell'e-policy e conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC nella promozione di comportamenti sicuri, sicurezza online e protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

Ruoli e responsabilità nell'implementazione dell'ePolicy

L'implementazione dell'ePolicy all'I.C. Settimo San Pietro è un processo corale che vede coinvolte diverse figure strategiche, coordinate per garantire la sicurezza digitale e l'attuazione delle linee guida del PTOF 2025-2028 e dei piani PNRR (DM 65 e DM 66).

A. Figure di Coordinamento e Governance

- Dirigente Scolastico: Promuove l'ePolicy, assicura le risorse necessarie per la formazione e supervisiona la gestione dei casi critici in sinergia con il territorio (es. PLUS 21).
- Referente per il contrasto al Bullismo e Cyberbullismo: Coordina le azioni di prevenzione, gestisce le segnalazioni e collabora con il Team per l'Innovazione per il monitoraggio del benessere digitale.
- Animatore Digitale e Team per l'Innovazione: Responsabili dell'attuazione delle misure tecnologiche e della formazione del personale sulla transizione digitale (DM 66/2023). Supportano la didattica innovativa legata a progetti come l'Arca del Tempo.

B. Personale Scolastico

- Docenti: Integrano l'ePolicy nella didattica quotidiana e nel Curricolo di Educazione Civica. Monitorano il comportamento degli studenti online e sono i primi referenti per l'ascolto di situazioni di disagio. Utilizzano gli strumenti STEM (DM 65/2023) in modo sicuro e responsabile.

- Personale ATA: Partecipa alla formazione sulla sicurezza dei dati e supporta la vigilanza sul corretto utilizzo dei dispositivi scolastici negli spazi comuni.

C. Comunità Educante: Studenti e Famiglie

Soggetto	Responsabilità Chiave
Studenti	Rispettare la Netiquette, custodire le proprie credenziali @scuolasettimo.edu.it e non ignorare eventuali episodi di abuso digitale, ma agire di conseguenza.
Genitori	Collaborare con la scuola firmando il Patto di Corresponsabilità, monitorare l'uso dei dispositivi a casa e partecipare agli incontri di formazione proposti (anche tramite il Centro Famiglia).

D. Supporto Specialistico

In conformità con le scelte strategiche del PTOF, l'Istituto si avvale del supporto del Responsabile della Protezione dei Dati (RPD) per gli aspetti legali e dello Psicologo Scolastico per il supporto emotivo, se previsto da progetti e finanziamenti garantendo una protezione a 360° per tutti gli alunni e per tutto il personale scolastico.

1.3 Integrazione ePolicy nei documenti scolastici

(Il paragrafo spiega in che modo integrare il documento nel Regolamento dell'Istituto Scolastico da aggiornare con specifici riferimenti all'E-policy, così come nel RAV e all'interno del Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto).

La trasversalità dell'ePolicy rende necessaria una sua integrazione nell'ambito dei documenti che disciplinano il funzionamento dell'Istituto Scolastico.

Il Regolamento dell'Istituto scolastico, che rappresenta il principale punto di riferimento normativo, dovrà essere aggiornato in modo tale da dare contezza dell'adozione dell'ePolicy, e richiamare le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione in ambiente scolastico.

Anche il **Patto di Corresponsabilità educativa** tra scuola e famiglia dovrà essere integrato con gli opportuni riferimenti all'ePolicy, puntualizzando, da un lato l'impegno dell'Istituto ad organizzare eventi formativi/informativi a beneficio dei genitori, e dall'altro l'impegno di questi ultimi a partecipare in maniera proattiva a tali eventi.

Il **Piano Triennale dell'Offerta Formativa**, per la sua funzione di carta d'identità culturale e progettuale delle istituzioni scolastiche, nel quale si esplicita la progettazione curricolare, extracurricolare, educativa e organizzativa che le singole scuole adottano nell'ambito della loro autonomia, deve contenere anche le progettualità relative ad azioni media educative legate al percorso di ePolicy.

Così come il PTOF è il risultato di una consapevole concertazione fra le componenti delle istituzioni scolastiche (Dirigente Scolastico, docenti, alunni, genitori) e fra queste e il territorio, il patto di corresponsabilità rappresenta l'assunzione di responsabilità da parte di tutti coloro che svolgono un ruolo attivo nella Comunità educante.

Il Regolamento d'Istituto viene aggiornato con specifici riferimenti all'E policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

La presente E-policy va quindi ad aggiungersi ed integrare i regolamenti già esistenti.

Integrazione dell'ePolicy nei documenti scolastici

L'ePolicy non è un documento isolato, ma costituisce un pilastro fondamentale dell'identità educativa dell'I.C. Settimo San Pietro. In coerenza con il PTOF 2025-2028, essa si integra e si coordina con i principali atti formali dell'Istituto per garantire una strategia digitale coerente e condivisa.

A. Collegamento con i documenti chiave

Documento	Modalità di Integrazione
PTOF 2025-2028	L'ePolicy declina operativamente le priorità strategiche relative alla transizione digitale (DM 66) e alle competenze STEM (DM 65).
Regolamento di Istituto	Le norme di comportamento digitale e le PUA (Politiche di Utilizzo Accettabile) diventano parte integrante delle regole di convivenza civile.
Patto di Corresponsabilità	Include l'impegno reciproco tra scuola e famiglia per un uso etico dei dispositivi e la tutela della privacy.
Curricolo di Educazione Civica	Le unità di apprendimento sulla cittadinanza digitale sono programmate in base ai contenuti dell'ePolicy.

B. Inclusione e Personalizzazione (BES)

L'ePolicy si raccorda con i Piani Didattici Personalizzati (PDP) e i Piani Educativi Individualizzati (PEI). Per gli alunni con Bisogni Educativi Speciali presenti nell'Istituto, l'ePolicy garantisce che l'uso delle tecnologie sia finalizzato all'abbattimento delle barriere all'apprendimento, definendo l'uso legittimo di strumenti compensativi digitali anche in classe.

C. Progettualità PNRR e Territoriale

L'integrazione si estende ai progetti specifici che caratterizzano l'Istituto:

- Protocollo con PLUS 21: L'ePolicy recepisce le procedure di intervento concordate con i servizi territoriali per la prevenzione del disagio.
- Progetto Arca del Tempo: Le linee guida sulla proprietà intellettuale e la privacy contenute nell'ePolicy regolano la produzione e pubblicazione di contenuti digitali sul patrimonio archeologico locale (Cuccuru Nuraxi).

D. Diffusione e Trasparenza

Per assicurare la massima efficacia, l'ePolicy è pubblicata sul sito istituzionale nella sezione dedicata alla trasparenza e alla didattica digitale. Ogni aggiornamento del PTOF comporta una revisione dell'ePolicy per assicurarne il costante allineamento agli obiettivi educativi della scuola.

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

1. il curricolo sulle competenze digitali per la comunità educante (il DigComp2.2);
2. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con relative informative;
3. Come comunicare e condividere l'epolicy con gli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).

1. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con relative informative;

L'efficacia dell'ePolicy è direttamente proporzionale a livello di conoscenza e diffusione all'interno della comunità scolastica ivi comprese le famiglie. Il documento rappresenta il canale interno privilegiato per informare, responsabilizzare e collaborare sui temi della rete e delle tecnologie a scuola con l'intera comunità scolastica.

In tal senso, il documento è accompagnato da versioni, allegate e sintetiche, all'interno delle quali sono individuati gli elementi principali del documento; una versione è diretta agli studenti ed una è diretta alle famiglie con un linguaggio e una presentazione dei contenuti adeguata, flessibile e chiara. La versione sintetica rivolta agli studenti è inserita all'interno delle attività didattiche dell'educazione alla cittadinanza mentre la versione per le famiglie è consegnata nel corso dei colloqui scuola-famiglia.

Il documento è altresì pubblicato sul sito della scuola ed inserito nel Patto di corresponsabilità.

2. Come comunicare e condividere l'ePolicy con gli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).

La presenza dell'ePolicy nell'Istituto scolastico è garanzia, per il territorio, della presenza di un presidio informato, sensibile e attento sulla rete e le tecnologie in relazione con i più giovani.

In questo senso l'Istituto può rappresentare per le Istituzioni del territorio, le aziende, e le realtà del Terzo Settore un luogo di confronto privilegiato e di sperimentazione per tutti coloro che intendono costruire progetti di cittadinanza digitale rivolte ai più giovani.

A tal fine l'adozione dell'ePolicy è comunicata all'USR di riferimento e al Municipio (servizi istruzione e servizi sociali) attraverso gli allegati sintetici progettati che indicano gli elementi del documento e le prospettive per la comunità.

CONDIVISIONE E COMUNICAZIONE AGLI STUDENTI E ALLE STUDENTESSE

Tutti gli alunni saranno informati che l'uso di Internet e di ogni dispositivo digitale all'interno dell'Istituto è subordinato all'autorizzazione da parte degli insegnanti (vedi Regolamento Disciplinare alunni) e che l'accesso e l'uso del laboratorio di informatica, sito al pian terreno della Scuola Secondaria di I grado, sono disciplinati dal Regolamento approvato dal Collegio dei Docenti in data 23/10/2019 e successive modifiche ed integrazioni, per la sicurezza on-line è stato anche pubblicato nel laboratorio di informatica con accesso a Internet.

CONDIVISIONE E COMUNICAZIONE AL PERSONALE SCOLASTICO

La linea di condotta dell'Istituto in materia di sicurezza per l'utilizzo delle tecnologie digitali e di Internet sarà discussa negli

organi collegiali e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito Istituzionale. Tutto il personale sarà reso consapevole del fatto che il traffico in Internet può essere monitorato, che si potrà risalire al singolo utente registrato e che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

Condivisione e comunicazione dell'ePolicy

Affinché l'ePolicy sia uno strumento vivo e conosciuto da tutta la comunità scolastica, l'I.C. Settimo San Pietro adotta strategie di comunicazione differenziate e costanti. In linea con il PTOF 2025-2028, la condivisione del documento è il primo passo per costruire una cultura della responsabilità digitale.

A. Modalità di Diffusione

L'Istituto utilizza i seguenti canali per garantire la massima conoscibilità del documento:

- Sito Web Istituzionale: Pubblicazione dell'ePolicy in una sezione dedicata e facilmente accessibile, correlata all'area "Regolamenti" e "Innovazione Digitale".
- Registro Elettronico: Invio di una notifica a tutte le famiglie e al personale all'inizio di ogni anno scolastico per segnalare la disponibilità del documento aggiornato.
- Account Istituzionali: Invio del documento in formato digitale agli indirizzi @scuolasettimo.edu.it di studenti e docenti.

B. Azioni di Sensibilizzazione (Piano di Comunicazione)

Destinatari	Strumenti di Comunicazione
Studenti	Presentazione dell'ePolicy durante le ore di Educazione Civica e nei laboratori STEM; creazione di infografiche semplificate affisse nei locali della scuola.
Genitori	Incontri tematici organizzati in collaborazione anche con il PLUS 21 ed eventuale Sportello d'Ascolto; informativa sintetica durante le assemblee di classe e/o progetti specifici (ad esempio "Genitori Digitali" dell'a.s.2025-26)
Docenti e ATA	Sessioni di formazione specifica nell'ambito del DM 66/2023; condivisione di materiali operativi nel Drive del Team Innovazione.

1.5 - I Piani di Azione dell'ePolicy

I piani di azione rappresentano il **programma triennale** di obiettivi che la scuola intende realizzare per promuovere la conoscenza delle regole e dei protocolli di intervento che sono stati adottati con il documento di ePolicy nella comunità scolastica.

Nei Piani di Azione sono riportati **gli impegni e le responsabilità** che la scuola si assume per promuovere sui temi dell'educazione civica digitale e dell'utilizzo sicuro e consapevole delle tecnologie e della rete:

- la rilevazione dei bisogni
- le iniziative informative e formative,
- la formazione di docenti, studenti e studentesse, e famiglie,
- il monitoraggio e la valutazione delle azioni (laddove possibile, anche all'interno del RAV);

I Piani di Azione si distinguono tra standard, comuni ad ogni scuola che ha adottato l'ePolicy, e autoprodotti ovvero definiti dalla scuola sulla base del proprio contesto territoriale e delle collaborazioni in essere con Istituzioni, associazioni e aziende.

1° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

- Realizzare un evento di presentazione dell'ePolicy ai docenti dell'Istituto;
- Realizzare un evento di diffusione dell'ePolicy in occasione degli Open Day e/o in occasione del SID dell'Istituto dedicato alle famiglie ed a studenti/esse;
- Diffondere l'ePolicy negli ambienti scolastici, a studenti e studentesse, docenti e famiglie attraverso le versioni friendly dell'ePolicy;

MODULO II

- Effettuare una rilevazione del fabbisogno formativo dei docenti sui temi dell'educazione civica digitale;
- Effettuare una rilevazione di interessi, bisogni e comportamenti delle famiglie sull' uso positivo del digitale;
- Avviare l'introduzione dell kit didattico come metodo e risorsa di lavoro in alcune classi pilota;

MODULO III

- Integrare l'ePolicy (norme, regolamenti e procedure) nei documenti dell'Istituto;
- Aggiornare la Politica d'Uso Accettabile (PUA) della scuola ed il regolamento BYOD dell'Istituto;

MODULO IV

- Definizione, a partire da quanto definito nell'ePolicy, delle procedure di segnalazione anche con linguaggio child/youth friendly perché possano essere accessibili a studenti e studentesse;
- Realizzare una reportistica delle segnalazioni ricevute e dei relativi esiti.

2° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

- Realizzare una formazione rivolta ai docenti dell'Istituto, sulla base dei risultati della rilevazione svolta nel corso del primo anno, anche attraverso il supporto di esperti/associazioni esterne o avvalendosi del percorso disponibile sul sito di Generazioni Connesse. La formazione deve coprire almeno il 60% del corpo docente.

MODULO II

- L'istituto utilizza il kit didattico come pratica metodologica e risorse a disposizione dei docenti per i percorsi di ECD attraverso la formazione specifica sviluppata per i docenti attraverso il sito di Generazioni Connesse;
- Effettuare una rilevazione di interessi, bisogni, comportamenti, abitudini di studenti e studentesse sui temi dell'educazione civica digitale;
- Realizzare una formazione rivolta agli studenti e alle studentesse attraverso il percorso previsto sulla piattaforma di Generazioni Connesse;
- Realizzare una formazione rivolta alle famiglie attraverso il percorso previsto sulla piattaforma di Generazioni Connesse

Visione e Missione dell'Istituto

In coerenza con il Piano Triennale dell'Offerta Formativa (PTOF) 2025-2028, l'I.C. Settimo San Pietro riconosce le Tecnologie dell'Informazione e della Comunicazione (TIC) come volano fondamentale per lo sviluppo di una cittadinanza attiva e consapevole. Lo scopo della presente ePolicy non è meramente regolativo, ma profondamente educativo e inclusivo.

L'Istituto si pone l'obiettivo di trasformare l'ambiente scolastico in un ecosistema digitale sicuro, dove l'innovazione tecnologica sia al servizio della personalizzazione dell'apprendimento, con particolare attenzione a:

- Equità e Inclusione: Garantire l'accesso e la partecipazione di alunni con Bisogni Educativi Speciali (BES) e supportare l'integrazione di studenti provenienti da contesti specifici, come le famiglie nomadi e la casa-famiglia locale.

- Sviluppo delle Competenze STEM (DM 65/2023): Integrare il pensiero computazionale e l'analisi dei dati nei percorsi curricolari per preparare gli studenti alle sfide del futuro.

- Benessere Digitale: Prevenire il disagio giovanile e promuovere un uso etico della rete, contrastando attivamente bullismo e cyberbullismo.

I Piani di Azione dell'ePolicy

I Piani di Azione declinano operativamente le strategie dell'Istituto per il triennio, sfruttando le risorse del PNRR Missione 4 e le sinergie con il territorio.

Area di Intervento	Azioni Specifiche (PTOF 2025-2028)	Partner/Risorse
Formazione Personale	Attuazione del DM 66/2023: percorsi formativi sulla transizione digitale per docenti e personale ATA.	Fondi PNRR
Prevenzione e Contrasto	Potenziamento dello sportello d'ascolto e laboratori di educazione all'affettività digitale.	PLUS 21 / Centro per la Famiglia
Didattica Innovativa	Progetti di realtà aumentata e digital storytelling legati ai beni archeologici locali (es. Cuccuru Nuraxi).	Arca del Tempo / CEAS
Cittadinanza Digitale	Aggiornamento del curricolo di Educazione Civica con moduli su Privacy, Identità Digitale e AI.	Team Innovazione

Integrazione con il Territorio

L'Istituto si impegna a collaborare stabilmente con gli enti locali per rendere l'ePolicy un patto di comunità. La sinergia con il PLUS 21 garantisce interventi specialistici e supporto legale in caso di incidenti critici online, mentre la collaborazione con

l'Amministrazione Comunale permette l'uso di spazi tecnologici avanzati per attività extrascolastiche.

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

- Kit Didattico
- Area formazione (per docenti, famiglie, studenti/sse con ePolicy)
- Canale Youtube (webinar, video-stimolo, serie per target differenti)
- Canale TikTok
- Canale Instagram
- Canale Facebook

Per dare concretezza alla ePolicy, I.C. di Settimo San Pietro si impegna a realizzare il progetto di Generazioni Connesse, che offre un ecosistema di risorse diversificate per supportare l'intera comunità educante.

Strumenti Operativi e Didattici

Kit Didattico: Una raccolta di schede, attività e percorsi pronti all'uso per i docenti, suddivisi per target di età, per integrare l'educazione civica digitale nelle lezioni.

Area Formazione: Piattaforme dedicate con percorsi specifici per:

Docenti**:** Approfondimenti metodologici e normativi.

Famiglie: Consigli pratici per la mediazione educativa a casa.

Studenti/esse: Percorsi interattivi legati al percorso di ePolicy della scuola

Canali di Comunicazione e Social

Generazioni Connesse utilizza un linguaggio multimediale per raggiungere gli utenti sui loro canali preferenziali:

Canale	Contenuti Principali
YouTube	Webinar per esperti, video-stimolo per la discussione in classe e serie tematiche.
TikTok	Video brevi e dal linguaggio immediato, ideali per il coinvolgimento diretto dei ragazzi.
Instagram	Infografiche, pillole informative e campagne di sensibilizzazione visiva.
Facebook	Approfondimenti per genitori e docenti, notizie su eventi e aggiornamenti normativi.

Cap 2 - Sensibilizzazione e prevenzione

2.1 - Sensibilizzazione e prevenzione

(Il capitolo raccoglie indicazioni su azioni formative per studenti/esse, famiglie e docenti con obiettivi a breve e lungo termine e riferimenti normativi (es legge 92 2019 su ECD). I rischi online andranno in appendice come glossario, sul sito come approfondimenti, sul kit didattico come attività.

La quotidianità in rete di ciascuno dei componenti della comunità scolastica - docenti, studenti e famiglie - deve essere caratterizzata da una consapevolezza critica delle caratteristiche degli ambienti e dei servizi online affiancata alle competenze per vivere al meglio il mondo connesso.

In questa direzione l'ePolicy è un documento che sviluppa azioni e interventi con l'obiettivo di raggiungere l'intera comunità scolastica e promuovere, ciascuno secondo il proprio ruolo, una cittadinanza digitale composta dalla conoscenza dei diritti in rete, dei rischi e delle opportunità per una partecipazione attiva e responsabile nella rete.

Sensibilizzazione e prevenzione

In linea con le priorità strategiche del PTOF 2025-2028, l'Istituto Comprensivo di Settimo San Pietro pone il benessere psicofisico degli studenti al centro dell'azione educativa. La sensibilizzazione e la prevenzione non sono considerate attività isolate, ma parte integrante del curricolo di Educazione Civica Digitale e dei progetti PNRR (DM 65 e DM 66).

Strategie di Sensibilizzazione e Prevenzione

L'Istituto adotta un approccio sistemico che coinvolge l'intera comunità educante (studenti, docenti e famiglie) attraverso le seguenti direttrici:

A. Interventi per gli Studenti

- Cittadinanza Digitale Attiva: Integrazione nei percorsi curricolari di moduli dedicati alla gestione dell'identità online, alla privacy e al contrasto dell'Hate Speech.
- Sviluppo delle Life Skills: Potenziamento delle competenze trasversali per aiutare gli alunni a gestire le pressioni del gruppo dei pari online e offline.
- Laboratori STEM (DM 65/2023): Utilizzo critico della tecnologia per la verifica delle fonti, per distinguere tra informazione e manipolazione (fake news).
- Progetto Arca del Tempo : Promozione di un uso positivo dei social media attraverso la narrazione digitale del patrimonio storico-archeologico locale (Cuccuru Nuraxi).

B. Formazione per il Personale (DM 66/2023)

Il Piano di Formazione dell'Istituto prevede percorsi specifici sulla transizione digitale e sulla gestione dei rischi online,

finalizzati a:

- Riconoscere precocemente segnali di disagio (cyberbullismo, isolamento sociale, vamping).
- Utilizzare strumenti di monitoraggio e segnalazione in conformità con le linee guida ministeriali.
- Implementare metodologie didattiche innovative che favoriscano l'inclusione di alunni BES attraverso il digitale.

C. Coinvolgimento delle Famiglie

L'ePolicy promuove l'alleanza educativa tra scuola e famiglia attraverso:

Iniziativa	Descrizione	Collaborazione
Scuola per Genitori	Incontri di formazione sull'uso consapevole dei social media e del gaming online.	PLUS 21 / Centro Famiglia
Sportello d'Ascolto	Supporto psicologico per la gestione di conflitti e criticità nate in ambiente digitale.	Psicologo Scolastico
Patti di Corresponsabilità	Aggiornamento dei contratti formativi con focus specifico sul comportamento digitale.	Consiglio di Istituto

D. Sinergie con il Territorio

L'Istituto collabora attivamente con le forze dell'ordine e con i servizi socio-educativi comunali per interventi di prevenzione di secondo livello, mirati a gruppi specifici o a situazioni di rischio elevato già identificate nell'analisi del contesto territoriale.

2.2 - Il Curricolo Digitale

Per realizzare questo obiettivo l’istituto utilizza le risorse messe a disposizione a livello nazionale e internazionale.

Il DigComp 2.2, framework europeo sulle competenze digitali, permette di costruire una cornice precisa in cui inquadrare i temi e le corrispondenti competenze da proporre nell' Istituto non solo per gli studenti.

Al suo interno vengono identificati alcuni temi sui quali è costruita una proposta specifica per le famiglie e gli studenti (formazione). Tale cornice trova poi sviluppo specifico, per gli studenti, nel curricolo di educazione alla Cittadinanza Digitale previsto dalla L. 92/2019. Il curricolo prende forma attorno all’ePolicy e le attività didattiche sono legate al documento ed alle scelte dell’Istituto al suo interno.

Nel curricolo va previsto in ogni classe un appuntamento didattico specifico, calibrato sull’età degli alunni, e l’utilizzo dei kit didattici per favorire da parte degli studenti una maggiore conoscenza e consapevolezza delle finalità del presente documento.

I regolamenti e le attività sviluppate sul tema della prevenzione presenti nell'ePolicy sono parte, costante ma non esclusiva, delle azioni di disseminazione e sensibilizzazione descritte ed attuate dall’Istituto.

Il Curricolo Digitale

L'I.C. Settimo San Pietro adotta un Curricolo Digitale verticale che attraversa tutti gli ordini di scuola, dalla Scuola dell'Infanzia alla Secondaria di Primo Grado. In linea con il PTOF 2025-2028, il curricolo non si limita all'alfabetizzazione tecnica, ma mira a sviluppare competenze critiche legate alla cittadinanza, alla sicurezza e alla creatività digitale, integrando le risorse del PNRR (DM 65 e DM 66).

Aree di Competenza e Obiettivi Specifici

Il curricolo è strutturato per rispondere ai bisogni del contesto locale, valorizzando le eccellenze del territorio e garantendo l'inclusione di alunni BES.

Area del Curricolo	Focus I.C. Settimo S. Pietro	Progetti Correlati (PTOF)
Alfabetizzazione su dati e informazioni	Sviluppare la capacità di ricercare e valutare criticamente le fonti digitali (Fact-checking).	Laboratori STEM (DM 65/2023)
Comunicazione e Collaborazione	Uso consapevole di Google Workspace per il lavoro cooperativo e la Netiquette istituzionale.	Transizione Digitale (DM 66/2023)
Creazione di Contenuti Digitali	Digital Storytelling applicato alla storia locale e all'archeologia (Cuccuru Nuraxi).	Progetto Arca del Tempo
Sicurezza e Benessere	Protezione dei dati personali, prevenzione del cyberbullismo e gestione dell'identità digitale.	Collaborazione PLUS 21

Metodologie Didattiche

Per l'attuazione del curricolo, l'Istituto promuove metodologie attive che rendono l'alunno protagonista:

- Coding e Pensiero Computazionale: Introdotti sin dalla scuola dell'infanzia per sviluppare il problem solving.
- Didattica Digitale Integrata: Utilizzo di piattaforme e strumenti digitali per rendere le lezioni interattive e accessibili, supportando la personalizzazione per gli alunni BES.
- CLIL Digitale: Potenziamento delle competenze linguistiche attraverso l'uso di software e risorse in lingua straniera (in linea con il DM 65/2023).

Valutazione delle Competenze

La valutazione delle competenze digitali è integrata nella valutazione periodica di Educazione Civica. L'Istituto definisce traguardi di competenza specifici per ogni fine ciclo, monitorando non solo l'abilità tecnica ma soprattutto l'atteggiamento critico e responsabile verso lo strumento tecnologico.

2.3 - Il Kit Didattico

L'e-Policy prevede, a livello macro, un lavoro di lettura e d'intenti condivisi dall'intera comunità scolastica, a livello micro, invece, immagina che la singola classe lavori anche su tematiche direttamente collegate alla sicurezza in rete, ma

complesse e di non immediata ricaduta nelle programmazioni scolastiche (etica e digitale, algoritmi, datafication). A tal fine si è progettato e predisposto del materiale che possa funzionare sia da attivatore, sia d'accompagnamento ai docenti e agli studenti nella fase più delicata ed incisiva del processo di prevenzione: la lezione in classe.

Pertanto, il progetto Generazioni Connesse, a supporto del lavoro dell'e-Policy ha previsto per i docenti e studenti di ogni segmento scolare un nuovo Kit Didattico che contiene materiali per le lezioni e per il proprio aggiornamento, a partire dalla scuola d'infanzia fino alla secondaria di secondo grado. Il Kit può essere usato nella sua interezza oppure può essere oggetto di selezione e scelta, sulla base di quanto fatto dal docente.

Capitolo 2 - Sensibilizzazione e prevenzione

2.3 - Il Kit Didattico dell'Istituto

L'I.C. Settimo San Pietro, per supportare l'attuazione del Curricolo Digitale e le azioni di prevenzione del cyberbullismo, adotta un Kit Didattico multimodale. Questo set di strumenti è progettato per essere inclusivo e per valorizzare le risorse tecnologiche acquisite tramite il PNRR.

Componenti del Kit Didattico

Strumento	Finalità e Utilizzo (PTOF 2025-2028)	Target
Google Workspace for Education	Piattaforma principale per la collaborazione sicura, la condivisione di materiali e la creazione di classi virtuali.	Docenti e Studenti
Risorse STEM (DM 65/2023)	Software di coding, kit di robotica educativa e sensori per l'analisi dei dati scientifici.	Studenti (Infanzia/Primaria/Sec.)
Materiali Generazioni Connesse	Vademecum, video e schede didattiche per la prevenzione di cyberbullismo, sexting e grooming.	Comunità Scolastica
Digital Storytelling "Arca del Tempo"	Template e software per la creazione di contenuti multimediali sul patrimonio di Cuccuru Nuraxi.	Studenti

Modalità di Erogazione

- Integrazione Curricolare: Il kit non è un pacchetto separato, ma viene utilizzato dai docenti durante le ore di Educazione Civica e nelle discipline STEM.
- Accessibilità: Tutti i materiali digitali sono ottimizzati per i software compensativi in uso per gli alunni con disturbi specifici dell'apprendimento, garantendo che nessuno sia escluso dalla formazione sulla sicurezza online.
- Supporto Tecnico: L'Animatore Digitale e il Team per l'Innovazione (finanziati tramite DM 66/2023) forniscono assistenza ai docenti per l'integrazione efficace di questi strumenti nella didattica quotidiana.

Monitoraggio e Aggiornamento

Il Kit viene aggiornato annualmente per includere nuove risorse emerse dal monitoraggio dei bisogni (PLUS 21) e dalle innovazioni tecnologiche, assicurando che l'Istituto risponda sempre alle nuove sfide del web (es. Intelligenza Artificiale generativa).

Cap 3 - Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola

3.1 - Protezione dei dati personali e GDPR

La protezione dei dati personali delle persone fisiche costituisce un diritto fondamentale. L'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea e l'art. 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Le principali normative di riferimento sono il Regolamento Generale sulla Protezione dei Dati 2016/679 noto anche come GDPR, e il Dlgs 196/2003 conosciuto come Codice Privacy.

Il settore dell'istruzione è particolarmente impattato dalla tematica privacy in considerazione del fatto che gli Istituti Scolastici sono chiamati, necessariamente, a trattare un'enorme mole di dati personali.

Con l'entrata in vigore del GDPR è stato introdotto l'obbligo per ciascun Istituto scolastico di provvedere alla designazione di un Responsabile della protezione dei dati personali (RPD o DPO).

I principali obblighi in materia di protezione dei dati personali consistono nella definizione di un "organigramma privacy", nel rilascio dell'informativa al momento della raccolta dei dati e nella tenuta di un registro dei trattamenti.

Protezione dei dati personali e GDPR

L'I.C. Settimo San Pietro opera nel pieno rispetto del Regolamento UE 2016/679 (GDPR). In linea con il PTOF 2025-2028 e la transizione digitale avviata con il PNRR (DM 66/2023), la protezione dei dati non è solo un obbligo giuridico, ma una componente essenziale della sicurezza degli ambienti di apprendimento innovativi.

A. Figure di Riferimento e Governance

- Titolare del Trattamento: Il Dirigente Scolastico dell'I.C. Settimo San Pietro.
- Responsabile della Protezione dei Dati (RPD/DPO): L'Istituto si avvale di una figura professionale esterna specializzata (attualmente individuata nella SAEMA Informatica) per la consulenza e il monitoraggio del rispetto della normativa.
- Registro dei Trattamenti: La scuola mantiene costantemente aggiornato il registro delle attività di trattamento, che include la gestione degli account istituzionali, i registri elettronici e i dati relativi ai progetti PNRR.

B. Sicurezza della Piattaforma Istituzionale

L'Istituto utilizza la piattaforma Google Workspace for Education (dominio @scuolasettimo.edu.it). La gestione dei dati avviene secondo criteri di massima sicurezza:

- DPIA (Valutazione di Impatto): L'utilizzo della piattaforma è supportato da una specifica valutazione di impatto sulla protezione dei dati per garantire la tutela della privacy di studenti e personale.

- Autenticazione: L'accesso è consentito solo tramite credenziali personali. In linea con il piano di formazione DM 66, il personale è istruito sulla gestione sicura delle password e sulla prevenzione del phishing.

C. Gestione dei Dati nel PNRR e Progetti STEM

Con l'attivazione dei laboratori STEM (DM 65/2023) e l'uso di nuove strumentazioni digitali, l'Istituto garantisce che:

- Ogni software o app utilizzata nella didattica sia preventivamente verificata sotto il profilo della conformità GDPR.

- I dati raccolti durante le attività di laboratorio (es. sensori, robotica educativa) siano trattati esclusivamente per fini didattici e in forma anonimizzata laddove possibile.

D. Procedure in caso di Violazione (Data Breach)

In conformità con il Regolamento, l'Istituto adotta una procedura rigorosa in caso di perdita, distruzione o diffusione non autorizzata di dati:

Fase	Azione	Responsabile
1. Rilevazione	Segnalazione immediata di anomalie o perdite di dati.	Chiunque rilevi l'evento
2. Valutazione	Analisi della gravità del rischio per i diritti degli interessati.	DS / RPD
3. Notifica	Comunicazione al Garante Privacy entro 72 ore (se necessario).	Dirigente Scolastico

E. Consapevolezza per Studenti e Famiglie

L'Istituto promuove la cultura della protezione dei dati attraverso moduli specifici nel Curricolo di Educazione Civica, spiegando agli alunni il valore della propria identità digitale e i rischi legati alla sovraesposizione online (oversharing).

3.2 - Strumenti di comunicazione online (PUA)

La Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) è un documento che racchiude una serie di regole legate all'utilizzo della rete a scuola e a casa da parte di studenti e di tutto il personale (compresi i professionisti esterni che lavorano in contesto scolastico), integrante il DPS (Documento programmatico sulla Sicurezza). Il documento, che funge da raccordo, si compone di punti strategici riguardanti non solo i vantaggi di internet a scuola ma anche i rischi connessi all'online, nella valutazione di quei contenuti presenti in rete e di quelle azioni negative che possono comprometterne l'uso positivo. Fra queste attività: ricercare materiale non consono allo stile educativo della scuola; produrre vere e proprie azioni illecite; giocare online con la rete scolastica; violare la privacy e i diritti d'autore, etc... Nella Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) vengono definite, dunque, le regole di utilizzo fra tutti gli attori in gioco, nel rispetto dei dati sensibili di ciascuno, in particolar modo degli alunni e delle alunne.

Strumenti di comunicazione online e Politiche di Utilizzo Accettabile (PUA)

L'I.C. Settimo San Pietro adotta canali di comunicazione digitale differenziati per finalità, garantendo la sicurezza dei dati e la trasparenza istituzionale. Coerentemente con il PTOF 2025-2028, la scuola promuove l'uso di questi strumenti per rafforzare la comunità educante.

A. Canali di Comunicazione Ufficiali

- Sito Web Istituzionale: Costituisce il principale canale di informazione pubblica e trasparenza amministrativa.
- Registro Elettronico (AXIOS): Strumento esclusivo per le comunicazioni scuola-famiglia relative alla didattica, voti, assenze e circolari.
- Email Istituzionale (@scuolasettimo.edu.it): Unica modalità autorizzata per lo scambio di informazioni tra personale, studenti e amministrazione. In linea con il DM 66/2023, il personale è formato sull'uso professionale e sicuro della posta elettronica.

B. Google Workspace for Education e Ambienti di Apprendimento

La piattaforma Google Workspace è l'ambiente protetto dedicato alla didattica digitale integrata. Le regole di utilizzo (PUA) prevedono:

- Uso Didattico: Le classi virtuali (Classroom) e gli strumenti di Meet sono riservati esclusivamente ad attività coordinate dai docenti.
- Collaborazione Inclusiva: Gli strumenti di condivisione sono configurati per supportare gli alunni BES, facilitando la cooperazione peer-to-peer in ambienti sicuri.
- Divieto di Chat Private: La comunicazione tra studenti all'interno della piattaforma deve avvenire esclusivamente per scopi didattici e sotto la supervisione dei docenti.

C. Policy per la messaggistica istantanea e Social Media

In linea con le azioni di prevenzione del cyberbullismo, l'Istituto stabilisce che:

Strumento	Regole di Utilizzo (PUA)
WhatsApp / Telegram	L'uso di gruppi di messaggistica per scopi scolastici è sconsigliato. Le comunicazioni ufficiali passano esclusivamente per il Registro o l'Email.
Social Network Scolastici	La pagina Facebook dell'Istituto è gestita dal Team Facebook composto da tre docenti, uno per ogni ordine scolastico, e utilizzata solo per scopi divulgativi di eventi e attività didattico-laboratoriali riguardanti la scuola.
Immagini e Video	È vietata la pubblicazione di immagini o video di studenti e personale senza specifico consenso informato depositato agli atti.

D. Responsabilità e Sanzioni

L'inosservanza delle Politiche di Utilizzo Accettabile (PUA) comporta l'applicazione delle sanzioni disciplinari previste dal Regolamento di Istituto e dallo Statuto delle Studentesse e degli Studenti, proporzionalmente alla gravità dell'infrazione

digitale commessa.

3.3 - BYOD

La presente ePolicy conterrà indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device"). Risulta infatti fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

BYOD: Bring Your Own Device (Uso di dispositivi personali)

L'I.C. Settimo San Pietro riconosce il valore delle tecnologie mobili come strumenti in grado di favorire la personalizzazione dell'apprendimento e lo sviluppo delle competenze digitali. In linea con il PTOF 2025-2028 e le linee guida sulla Didattica Digitale Integrata, l'Istituto regolamenta l'uso di dispositivi personali (PC, tablet, smartphone) secondo il modello BYOD.

A. Finalità Didattiche e Inclusione

L'uso dei dispositivi propri è consentito esclusivamente per fini educativi e sotto la diretta supervisione del docente. In particolare:

- Supporto all'Inclusione: Il BYOD è una risorsa fondamentale per gli alunni con Bisogni Educativi Speciali (BES), che possono utilizzare i propri dispositivi come strumenti compensativi personalizzati (sintesi vocale, mappe concettuali, software specifici).
- Progetti Territoriali: L'uso di smartphone e tablet personali è incentivato per attività di ricerca sul campo e digital storytelling.
- Laboratori STEM: Integrazione con la strumentazione acquisita tramite il DM 65/2023 per attività di coding e analisi dati.

B. Regole di Accesso e Sicurezza

Ambito	Regola Comportamentale
Connettività	L'accesso alla rete Wi-Fi di Istituto è consentito solo tramite autenticazione con account @scuolasettimo.edu.it e previo filtraggio dei contenuti.
Responsabilità	La scuola non risponde di furti, smarrimenti o danni ai dispositivi personali portati a scuola. La custodia è a carico dello studente.
Privacy e Riprese	È tassativamente vietato registrare audio, scattare foto o girare video senza l'esplicita autorizzazione del docente e per soli fini didattici.

C. Il Ruolo del Docente e la Formazione

Nell'ambito del piano di formazione DM 66/2023, i docenti dell'Istituto sono formati per:

- Gestire efficacemente le dinamiche di classe in presenza di dispositivi personali.
- Educare gli studenti alla "Netiquette" e all'uso critico della rete durante le sessioni BYOD.
- Monitorare che l'uso del dispositivo non diventi fonte di distrazione o di esclusione sociale.

D. Sanzioni per uso improprio

L'utilizzo del dispositivo personale al di fuori delle attività didattiche autorizzate o per scopi contrari alla dignità delle persone (cyberbullismo, diffusione di contenuti non idonei) comporta l'immediato ritiro del dispositivo e l'applicazione delle sanzioni disciplinari previste dal Regolamento di Istituto.

Cap 4 - Segnalazione e gestione dei casi

4.1 - Cosa Segnalare

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire). Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Queste, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola.

Nelle procedure sono indicate le figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso, nonché le modalità di coinvolgimento del Dirigente Scolastico e del Referente per il contrasto al bullismo e al cyberbullismo. Inoltre, la scuola individua le figure che costituiranno un team preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica. La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

A seguire, le problematiche a cui fanno riferimento le procedure allegate:

Cyberbullismo: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).

Adescamento online: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

Sexting: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere, per quanto possibile, la rimozione del materiale on-line e il blocco della sua diffusione per mezzo dei dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete.

Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;
- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

Cosa Segnalare

L'I.C. Settimo San Pietro promuove una cultura della responsabilità condivisa. Coerentemente con il PTOF 2025-2028, che pone tra le priorità strategiche il contrasto al bullismo e il benessere psicofisico, l'Istituto definisce con chiarezza gli eventi che richiedono una segnalazione tempestiva.

A. Tipologie di eventi da segnalare

Devono essere oggetto di attenzione e segnalazione tutti i comportamenti online che violano la dignità della persona, la sicurezza dei dati o il regolamento d'Istituto, tra cui:

- Cyberbullismo e Molestie: Diffusione di messaggi offensivi, isolamento intenzionale da gruppi di classe o creazione di profili falsi per deridere compagni o personale.
- Hate Speech: Discorsi d'odio rivolti a singoli o gruppi, con particolare attenzione alla tutela dei gruppi fragili presenti nell'Istituto (studenti con BES 17%, minoranze etiche, ecc.).
- Uso Improprio di Immagini: Ripresa o diffusione non autorizzata di foto/video durante le lezioni o nei laboratori STEM e durante le uscite didattiche.
- Violazioni della Privacy (Data Breach): Accesso non autorizzato ad account istituzionali @scuolasettimo.edu.it o smarrimento di dispositivi contenenti dati sensibili.
- Contenuti Inappropriati: Visualizzazione o condivisione di materiale violento, pornografico o inneggiante a condotte pericolose.

B. Criteri di Valutazione della Gravità

L'Istituto adotta i seguenti criteri per valutare l'entità del caso:

Criterio	Descrizione
Persistenza	L'atto è isolato o si ripete nel tempo?
Ampiezza	Quante persone sono coinvolte o hanno visualizzato il contenuto?
Intenzionalità	C'era la volontà di arrecare un danno o un disagio psicologico?

C. Il ruolo della "Segnalazione Protettiva"

L'Istituto educa gli studenti, attraverso il Curricolo di Educazione Civica, a distinguere la segnalazione "protettiva" (fatta per aiutare una vittima o se stessi) dalla "delazione". Il fine ultimo è la tutela del clima di classe e del benessere individuale, come sottolineato negli obiettivi di miglioramento del PTOF.

D. Rilevazione tramite Sportello d'Ascolto

Si sa che spesso i casi di disagio digitale emergono durante le attività dello Sportello d'Ascolto psicologico. In questi casi, lo specialista opera in sinergia con il Referente Cyberbullismo e il Dirigente Scolastico per attivare le procedure previste nel Capitolo 5, garantendo la massima riservatezza.

4.2 - Quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale (ex art. 357 c.p.) in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Il Codice Penale Italiano, all'art. 357, definisce il pubblico ufficiale come colui che esercita una "pubblica funzione legislativa, giudiziaria o amministrativa". Questa definizione si estende ai docenti nel momento in cui sono impegnati nell'esercizio delle loro funzioni all'interno degli istituti scolastici.

La Corte di Cassazione, con la sentenza n. 15367/2014, ha ribadito la qualifica di pubblico ufficiale per l'insegnante, estendendo tale riconoscimento non solo alla tenuta delle lezioni, ma anche a tutte le attività connesse. Questo include, ad esempio, gli incontri con i genitori degli allievi.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite da un team di docenti composto da:

1. Dirigente
2. Docente referente,
3. L'animatore digitale (secondo il Piano Nazionale per la Scuola Digitale, abbreviato in PNSD, introdotto dalla Legge 107/2015)
4. Referente bullismo (ex. Legge Italiana Contro il Cyberbullismo, l. 71/2017
5. Altri docenti già impegnati nelle attività di promozione dell'educazione civica.

Le situazioni di pregiudizio presunto o reale possono richiedere il supporto e l'intervento di esperti esterni alla scuola.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due macro - casi:

CASO A (SOSPETTO) – Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l'obiettivo di allertare il Dirigente . La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, il Dirigente e i docenti coinvolti procedono alla valutazione del caso (valutare l'invio o meno della relazione agli organi giudiziari preposti) e agiscono tramite percorsi di sensibilizzazione.

CASO B (EVIDENZA) – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria

classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l'obiettivo di allertare il Dirigente. La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, si procede alla valutazione approfondita e alla verifica di quanto segnalato, avviando (se appurato la rilevanza penale) la procedura giudiziaria con denuncia all'autorità giudiziaria per attivare un procedimento penale.

Qualora si rilevasse un fatto riconducibile alla fattispecie di reato, l'insegnante - nel ruolo di pubblico ufficiale – non deve procedere con indagini di accertamento ma ha sempre l'obbligo di segnalare l'evento all'autorità giudiziaria. (ex. l. 71/2017). Con autorità competente si intendono:

- Procure Ordinarie: nel caso in cui il minore/i sia la vittima/e e il presunto autore del reato sia maggiorenne,
- Procura Minorile: in caso il presunto autore del reato sia minorenne.

Vi è anche l'obbligatorietà della segnalazione delle situazioni di pregiudizio a carico dei minori: L. 216/1991: per le situazioni di grave rischio l'istituzione scolastica è tenuta alla segnalazione delle medesime. Per pregiudizio si intende una condizione di rischio o grave difficoltà che provocano un danno reale o potenziale alla salute, alla sopravvivenza, allo sviluppo o alla dignità del bambino, nell'ambito di una relazione di responsabilità, fiducia o potere.

La segnalazione come da procedura interna è il primo passo per aiutare un minore che vive una situazione di rischio o di grave difficoltà e va intesa come un momento di condivisione e solidarietà nei confronti del minore. La mancata segnalazione costituisce, infatti, omissione di atti d'ufficio (art.328 C.P.).

Può essere utile, valutando accuratamente ciascuna situazione, attivare colloqui individuali con tutti i minori coinvolti, siano essi vittime, testimoni e/o autori. È importante considerare il possibile coinvolgimento dei genitori e di coloro incaricati della tutela dei minori coinvolti. L'intervento va indirizzato valutando l'eventuale impatto educativo e/o il contesto emotivo senza discriminare tra vittime, testimoni e/o autori.

Prevedere possibili incontri di mediazione tra i minori coinvolti vanno ponderati con la consapevolezza del loro stato emotivo, anche e in base agli elementi raccolti in merito del fatto/episodio avvenuto (elementi che si dovrebbero valutare di caso in caso). Importante è prevedere il coinvolgimento dei genitori sia della vittima che del bullo (ove possibile).

Anche i genitori devono e possono segnalare casi di sospetto o evidenza dei fenomeni, segnalarlo al Dirigente, o al docente coordinatore di classe o referente di istituto oppure direttamente al team antibullismo attraverso apposita procedura che definisce l'istituto (mail ad hoc, tramite gli uffici e postazioni specifiche, etc...).

Gli insegnanti e i genitori, come studenti e studentesse, si possono rivolgere alla Helpline del progetto Generazioni Connesse, al numero gratuito 19696, attraverso la chat disponibile sul sito o tramite chat WhatsApp per ricevere supporto e consulenza. Per tutti i dettagli, il riferimento è agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

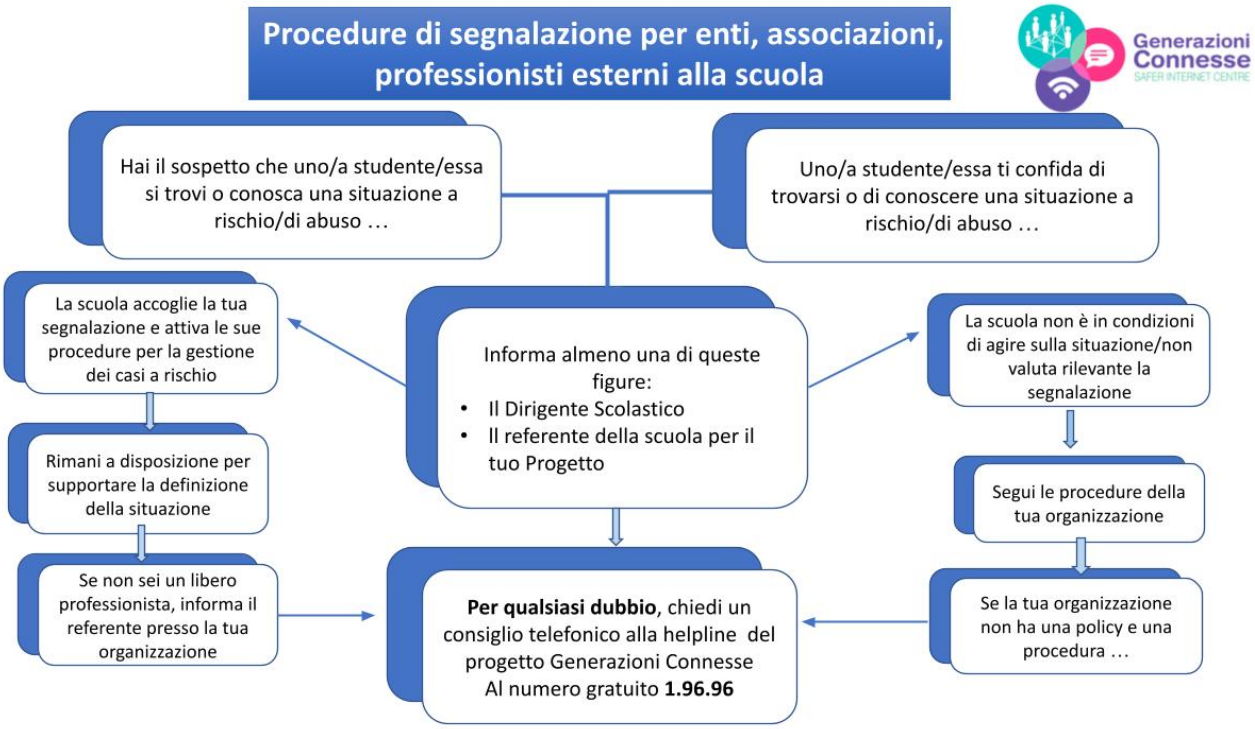
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola; sportello di ascolto con professionisti; docente referente per le segnalazioni.

In particolare, sarebbe utile che la scuola attivi un sistema di segnalazione utile anche al monitoraggio dei fenomeni dal quale partire per integrare azioni didattiche preventive e giornate di sensibilizzazione, insieme agli Enti/Servizi presenti sul

territorio di riferimento. Importante, altresì, immaginare e programmare percorsi di peer education per la prevenzione e il contrasto degli agiti.

Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle Linee di Orientamento per la prevenzione e il contrasto dei fenomeni di Bullismo e Cyberbullismo del MI (Ministero dell'Istruzione) aggiornate al 2021, al Patto educativo di corresponsabilità e annessa appendice relativa agli impegni che le parti in causa dovranno assumere per l'espletamento efficace della DID e, in ultimo, al Piano scolastico per la Didattica Digitale Integrata, allegato al PTOF.

Procedure



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

Il docente ha evidenza che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Se non è già stato fatto, avvisa il referente per il cyberbullismo (e/o il team antibullismo) che attiva le procedure ("Corso 4" della piattaforma ELISA) e il Dirigente Scolastico.
Ricordare sempre che in base alla legge 71-2017:
A) Se c'è fattispecie di reato va fatta la segnalazione alle forze dell'ordine
B) Se non c'è fattispecie di reato.
Il DS (e/o il team antibullismo):
- informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto) su quanto accade e condividete informazioni e strategie.
- Informa i genitori di ragazzi/e infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy)
- Attiva il consiglio di classe.

A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnala alla Polizia Postale:
a) contenuto; b) modalità di diffusione.
Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).

Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

NELLE CLASSI
Il team antibullismo collabora coi docenti della classe per realizzare l'intervento nella classe:
a seconda della situazione valuta se
- affrontare direttamente l'accaduto o
- sensibilizzare la classe (vedi Corso 4 Piattaforma Elisa)
- trova il modo di supportare la vittima e di responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo

Il docente riceve una segnalazione (da un genitore, un altro studente …) o sospetta che stia accadendo qualcosa a uno/a studente/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Condividi con il referente o al team antibullismo: si attiva il processo di attenzione e valutazione a cura del referente.

Insieme si valuta se è il caso
- di avvisare il consiglio di classe;
- di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.

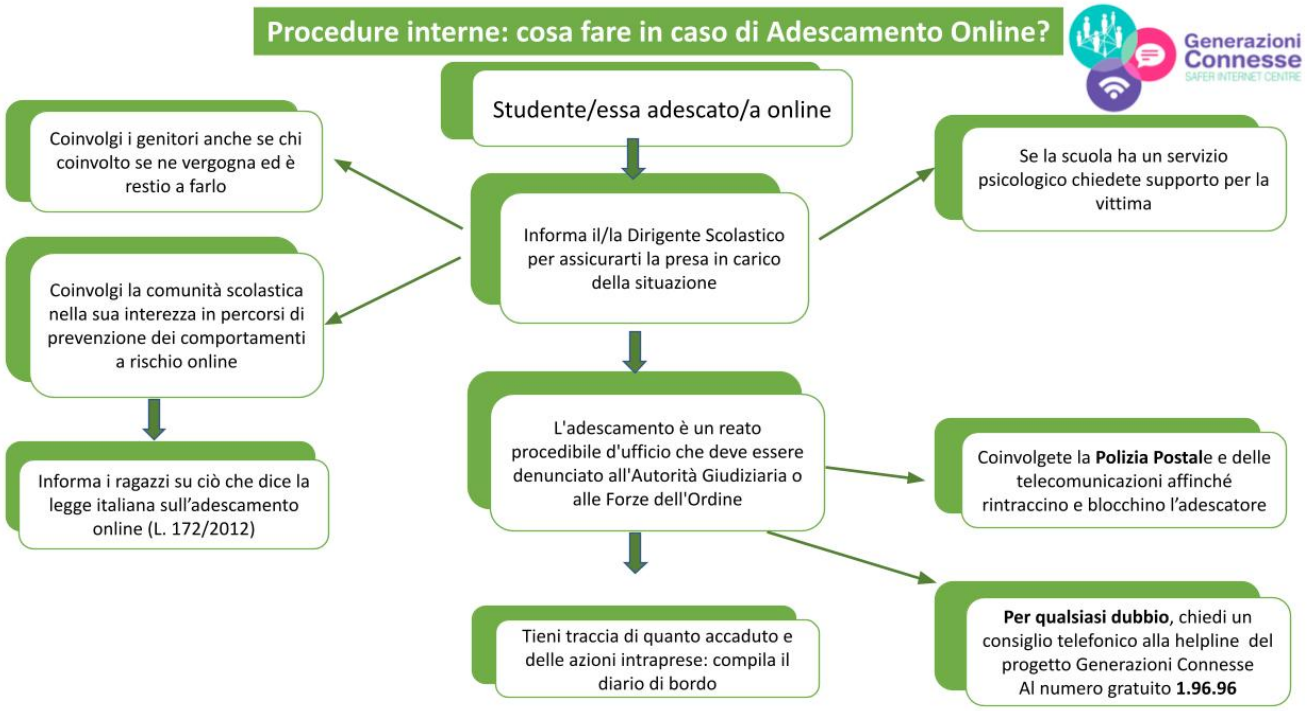
Se emergono evidenze passa allo schema successivo

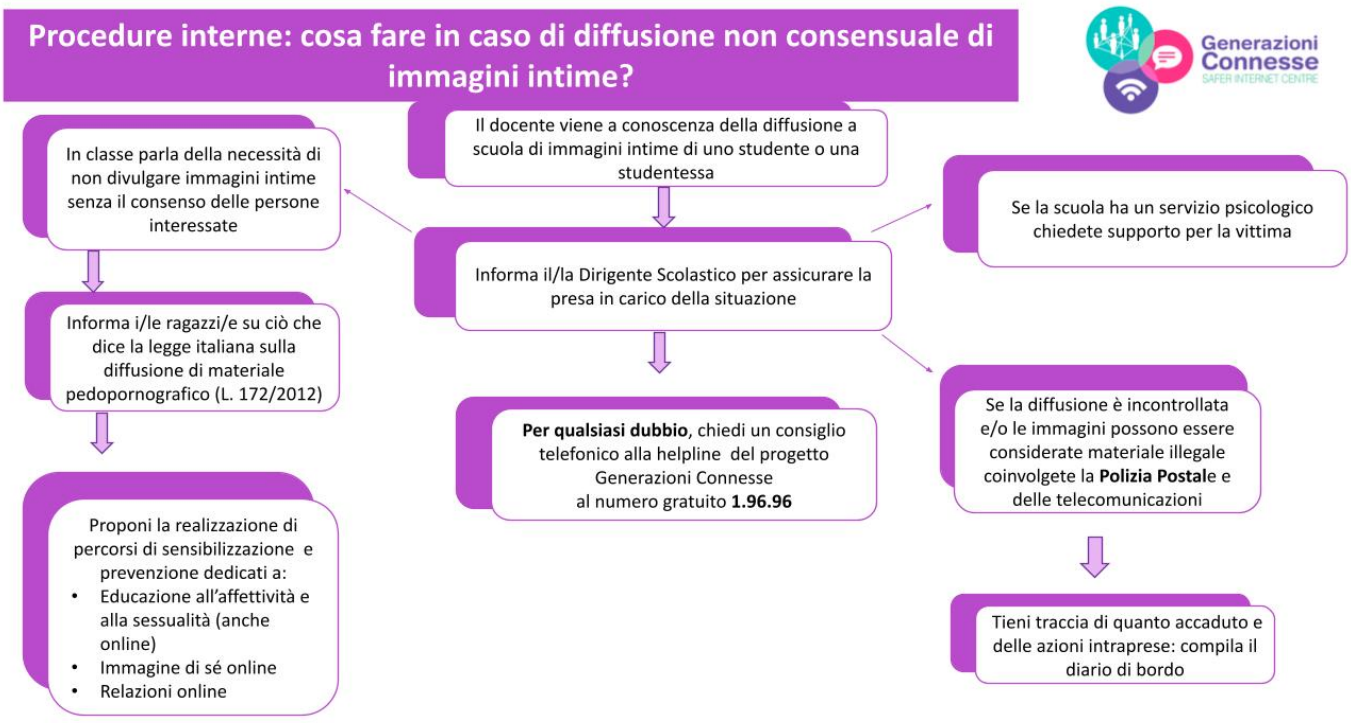
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

Scarica le linee di orientamento per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo

Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Ricorda a studenti/esse che possono chiedere in qualsiasi momento una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 o via chat





Quali strumenti e a chi rivolgersi

In conformità con il PTOF 2025-2028, l'Istituto ha definito procedure chiare e canali dedicati per garantire che ogni segnalazione sia gestita con la massima riservatezza e tempestività, tutelando il benessere di tutti gli studenti, con

particolare attenzione al 17% di alunni con Bisogni Educativi Speciali (BES).

A. Le Figure di Riferimento

All'interno dell'I.C. Settimo San Pietro, i nodi della rete di segnalazione sono:

- Referente per il contrasto al Bullismo e Cyberbullismo e team antibullismo : Figure incaricate di coordinare le azioni di prevenzione e gestire i flussi comunicativi dei casi rilevati.
- Il Dirigente Scolastico: Responsabile ultimo della gestione dei casi critici e dei rapporti con le autorità esterne.
- Il Team per l'Innovazione / Animatore Digitale: Supportano l'analisi tecnica in caso di violazioni della sicurezza informatica o degli account @scuolasettimo.edu.it.
- Lo Psicologo Scolastico (Sportello d'Ascolto) quando previsto: Punto di primo contatto per il disagio emotivo legato a dinamiche online.

B. Canali e Strumenti di Segnalazione

Strumento	Descrizione e Destinatario	Modalità
Colloquio Diretto	Modalità privilegiata per studenti e famiglie verso docenti di classe o Referente.	In presenza / Riservata
Sportello d'Ascolto	Accesso diretto allo psicologo per segnalare malessere legato a episodi online.	Prenotazione interna
Email Istituzionale	Segnalazione formale alla casella della scuola (o specifica del Referente).	Scritta
Scheda di Segnalazione	Modulo standardizzato (Allegato ePolicy) per la raccolta oggettiva dei fatti.	Cartacea / Digitale

C. La Rete Territoriale: PLUS 21

Nei casi in cui la problematica superi i confini scolastici o richieda un supporto specialistico aggiuntivo, l'Istituto attiva la collaborazione con il Centro per la Famiglia (PLUS 21). Questo partner territoriale offre consulenza psicologica, legale e mediazione familiare per gestire gli incidenti digitali che coinvolgono il contesto extra-scolastico.

D. Segnalazione Esterna (SIC e Polizia Postale)

L'ePolicy prevede, per i casi di particolare gravità (es. reati procedibili d'ufficio o adescamento), che la segnalazione venga inoltrata dal Dirigente Scolastico alle autorità competenti:

- Safer Internet Centre (Generazioni Connesse): Tramite la Helpline e il portale di segnalazione.
- Polizia Postale: Per reati telematici e violazioni gravi della privacy o della dignità dei minori.

E. Procedura per gli studenti: "Non restare in silenzio"

Nell'ambito del Curricolo di Cittadinanza Digitale, gli studenti vengono istruiti a non cancellare le prove (screenshot) e a rivolgersi immediatamente a un adulto di fiducia della scuola, garantendo loro che ogni segnalazione sarà trattata con cura e non darà luogo a ritorsioni.