Documento di ePolicy
I.C. “Taddeo Cossu” Teulada

VIA NINO BIXIO 34 – 09019 - TEULADA
Teulada (SU)- Sardegna
Data di approvazione: 19/12/2025

Cap 1 - Lo scopo della ePolicy

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)

Capitolo4 – 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

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'e Policy 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.

- 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.

ILDIRIGENTE 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;
- devetutelarelascuolaegarantireagliutentilasicurezzadinavigazioneutilizzandoadeguatisistemiinformaticie

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 PERL'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.

ILREFERENTEPERILBULLISMOECYBERBULLISMO

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

ILTEAMANTIBULLISMOEPERL'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 DirigenteScolastico,coordinatoredelTeamnellascuola,nelladefinizionedegliinterventidiprevenzioneenellagestionedei casi di bullismo e cyberbullismo che si possono presentare. Promuove inoltre la conoscenza e la consapevolezza del bullismoedelcyberbullismoattraversoprogettid'istitutochecoinvolganogenitori,studentietuttoilpersonaleecomunicaadalunni, famiglie e tutto il personale scolastico dell'esistenza del team, a cui poter fare riferimento per segnalazioni o richieste di informazioni sul tema.

IlTeam 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/LEDOCENTI

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.

RESPONSABILEDELLAPROTEZIONEDEIDATI

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

ILPERSONALEAMMINISTRATIVO,TECNICOEAUSILIARIO(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.

GLISTUDENTIELESTUDENTESSE

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,

IGENITORI/ADULTIDIRIFERIMENTO

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.

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,edall'altrol'impegnodiquestiultimiapartecipareinmanieraproattivaatalieventi.

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.

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 rivolti 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.

- 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 ATTIVITÀ 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 OpenDay 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 del 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° ANNODIATTIVITÀ CON L'EPOLICY

MODULOI

- 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 sulsito 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

---

- Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

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

Cap 2 – Sensibilizzazione e prevenzione

- 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.

- 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 curriculum digitale d'istituto è consultabile nell'apposita sezione del sito web della scuola.

-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,immaginachelasingolaclasselavorianchesutematichedirettamentecollegateallasicurezzainrete,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 KitDidattico 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.

Inoltre il team digitale ha predisposto un modulo formativo per le classi quinte della scuola primaria e tutte le classi della scuola secondaria di I grado dal titolo "Vademecum digitale studenti". Tale strumento è costituito da una presentazione informativasullemodalitàdiutilizzoresponsabiledelletecnologieinambitoscolasticoedauntestfinaledivalutazionedelle competenze acquisite, valutabile nell'ambito dell'insegnamento trasversale dell'educazione civica.

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

- 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.

Testo dell'informativa "Trattamento dei dati personali" - Istituto Comprensivo"Taddeo Cossu" Teulada

Ai sensi della normativa vigente in materia di protezione dei dati personali (Regolamento UE n. 679 del 2016), l'Istituto informa che i trattamenti dei dati personali forniti sono effettuati con correttezza e trasparenza, per fini leciti e tutelando la sua riservatezza ed i suoi diritti.

I trattamenti sono effettuati, anche con l'ausilio di mezzi informatici, per le seguenti finalità:

1. per i servizi scolastici, contabili ed amministrativi. Trattandosi di trattamenti necessari non è richiesto il suo consenso, tranne nel caso in cui siano conferiti dati particolari, cosiddetti sensibili. In caso di rifiuto a conferire i dati personali, non potremo fornirle i servizi richiesti. Il trattamento cesserà al termine del percorso scolastico, ma alcuni suoi dati personali potranno o dovranno continuare ad essere trattati per le finalità e con le modalità indicate nei punti successivi;

2. per adempiere ai vigenti obblighi scolastici, amministrativi, contabili e fiscali. Per tali finalità il trattamento è effettuato senza necessità di acquisire il consenso. I dati sono trattati dall'Istituto e dai nostri incaricati, e vengono comunicati all'esternosoloinadempimentoadobblighidilegge.Incasodirifiutoaconferireidatinecessaripergliadempimenti sopra indicati, non potremo fornirle i servizi richiesti. I dati acquisiti per tali finalità vengono da noi conservati per il tempo previsto dalle rispettive normative (10 anni, e anche oltre in caso di accertamenti);

3. per inviare messaggi (via telefono e posta elettronica) di aggiornamento sulle nuove attività o sui nuovi adempimenti oppure per ricordare scadenze o eventi. Per tale finalità, previa acquisizione del suo consenso, i suoi dati saranno conservati per il periodo massimo di due anni a decorrere dalla data dell'ultimo anno frequentato e non saranno comunicati a terzi. Potrà revocare il consenso in qualsiasi momento;

4. per l'organizzazione di attività extrascolastiche come gite, eventi, visite culturali. Per tale finalità i suoi dati saranno comunicati a terzi e conservati per il solo periodo necessario all'espletamento dell'attività. Potrà revocare il consenso in qualsiasi momento.

L'Istituto desidera inoltre informare che il Regolamento europeo le riconosce alcuni diritti, tra cui il diritto di accesso e di rettifica, di cancellazione o di limitazione, di opposizione al trattamento oltre al diritto alla portabilità dei dati, se ed in quanto applicabili (articoli da 15 a 22 del Regolamento UE n. 679 del 2016).

Può inoltre proporre reclamo all'autorità di controllo, secondo le procedure previste dalla normativa vigente.

Per qualsiasi ulteriore informazione, e per far valere i diritti a lei riconosciuti dal Regolamento europeo, potrà rivolgersi a:

Titolare del trattamento: Istituto Comprensivo "Taddeo Cossu" Teulada, Via Nino Bixio, 34 – 09019 Teulada (SU)

DS – caic82100n@istruzione.it

Responsabile del trattamento: DSGA - caic82100n@istruzione.it

Responsabile della Protezione dei Dati: Mario Mureddu mario.mureddu@muredduconsulting.com

https://trasparenza-pa.net/?codcli=SC15279&node=3608981

La scuola richiede alle famiglie l'autorizzazione alle riprese fotografiche e video a fini di pubblicazione o divulgazione sul sito e sui canali social dell'istituto attraverso la liberatoria presente sul diario scolastico. In nessun caso vengono pubblicati i volti riconoscibili degli studenti e delle studentesse.

In caso di divulgazione tramite Casa editrice e Progetto Podcast, viene proposta ai genitori tramite diario scolastico ulteriore liberatoria custodita dal referente di progetto.

- 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.

La scuola garantisce a tutti gli utenti il diritto a internet attraverso un'infrastruttura di rete adeguata al numero di studenti e in grado di supportare il traffico dati generato da un numero elevato di utenti. La connessione è in fibra ottica, è cablata sull'intero istituto ed è dotata di firewall gestito dal tecnico esterno designato.

Interventi periodici di manutenzione e verifica sono programmati dal DS in accordo con l'AD e/o il tecnico della scuola. Altre verifiche possono essere effettuate su segnalazione degli utenti.

La segreteria didattica, quella amministrativa, l'ufficio del DSGA e la presidenza sono connesse a rete LAN dedicata e a

server indipendente ubicato in un'aula appositamente predisposta all'interno dell'istituto, a sua volta connesso a server esterno per la sicurezza dei dati.

L'infrastruttura di rete nell'istituto è così organizzata:

Rete WI-FI: a cui sono connessi tutti i pc di classe e le LIM della scuola;
Rete WI-FI Didattica: a cui sono connessi docenti;
Rete LAN e WIFI Segreteria; a cui è connessa la segreteria.

Come da regolamento sull'uso delle TIC allegato, gli studenti si impegnano a: utilizzare la rete nel modo corretto, rispettare le consegne dei docenti, non scaricare materiali e software senza autorizzazione, non utilizzare unità rimovibili personali, segnalare immediatamente materiali inadeguati ai propri insegnanti.

Per ulteriori specifiche disposizioni si rimanda ai regolamenti scolastici.

I docenti si impegnano a: utilizzare la rete nel modo corretto, non utilizzare device personali se non per uso didattico, formare gli studenti all'uso della rete, dare consegne chiare e definire gli obiettivi delle attività, monitorare l'uso che gli studenti fanno delle tecnologie a scuola.

Tutte le componenti della scuola sono tenute a rispettare il **Regolamento sull'uso dei laboratori** redatto da AD e team digitale e affisso negli spazi interessati.
Tale regolamento viene qui riportato per esteso:

- L'accesso da parte delle classi o di gruppi di studenti nei laboratori è consentito solo con la presenza di un docente.
- GLI STUDENTI NON POSSONO PRELEVARE I DISPOSITIVI DA SOLI.
- È vietato mangiare o bere nei pressi dei dispositivi digitali o attrezzature specifiche.
- Le chiavi dei laboratori sono custodite presso la postazione dei Collaboratori Scolastici più vicina.

Prima di ogni attività:

- ricordare agli studenti che sui dispositivi della scuola bisogna ACCEDERE COME OSPITE e che non bisogna MAI SALVARE LE PROPRIE PASSWORD sui dispositivi della scuola.

Al termine di ogni attività:

- Accertarsi che gli studenti abbiano effettuato il LOGOUTdai dispositivi;
- contare i dispositivi per assicurarsi che siano tutti presenti e riporli nelle apposite postazioni di carica;
- lasciare i carrelli di ricarica chiusi;
- rimettere a posto sedie e tavoli nella disposizione originale;
- spegnere luci e touch panel;
- chiudere le porte a chiave;
- lasciare gli spazi puliti ed eliminare eventuali rifiuti;

- segnalare eventuali problemi al team digitale (e per la Secondaria sul documento condiviso con il tecnico “Problematiche informatiche”)

REGOLAMENTO PRENOTAZIONE LABORATORI E AULE DI USO COMUNE:

- I docenti dovranno utilizzare Google Calendar per prenotare i laboratori, seguendo il tutorial in fondo al presente documento.
- Nella prenotazione i docenti dovranno indicare: tipo di attività, classe e docente accompagnatore.
- È vietato prenotare l’aula sempre nella stessa ora per più di tre settimane consecutive, ad eccezione dei corsi extracurriculari.
- I docenti sono tenuti a rispettare gli orari di prenotazione, arrivando puntuali e terminando l’attività entro i tempi concordati.

I dispositivi vanno usati in presenza di almeno un docente formato per il loro utilizzo.

Come specificato nel Patto di corresponsabilità, la scuola si fa carico di tutte le precauzioni necessarie per garantire agli/lle studenti/esse l’accesso a materiale appropriato, ma allo stesso tempo non può essere responsabile per l’accesso autonomoda parte degli/lle studenti/esse a materiali inadeguati e potenzialmente dannosi trovati online.

La scuola adotta per tutto il personale e gli studenti la Suite **GOOGLE WORKSPACE**.

Tutti gli studenti hanno accesso ad una serie di servizi, tra i quali GMAIL (e-mail personale con spazio di archiviazione illimitato), Drive (spazio di archiviazione cloud senza limiti di spazio) e Classroom (classe virtuale).
I servizi offerti sono ESCLUSIVAMENTE per utilizzo scolastico e didattico.
L'utilizzo della Google Suite è indispensabile per realizzare l'azione didattica programmata nel PTOF d'Istituto.

I genitori/tutori devono concedere l’autorizzazione alla creazione dell’account e all’utilizzo di Google Workspace da parte dei figli. Nel momento in cui gli account degli studenti vengono creati e attivati, essi rimangono attivi per tutta la durata della permanenza nell'Istituto comprensivo.

I genitori sono responsabili della vigilanza sull'utilizzo degli account scolastici a casa e sui dispositivi personali degli studenti, in particolare sull’utilizzo degli account per finalità esclusivamente didattiche e in accordo con i docenti. È vietato, ad esempio, utilizzare il proprio account scolastico per registrarsi su piattaforme di gioco online o sui social network a uso personale. In caso di violazione l’account può essere sospeso dall’amministratore del dominio, e ripristinato una volta effettuato l’accertamento sull’utilizzo corretto dell’account.

Lo stesso avviene per gli account di docenti e personale della scuola.

Gli account scolastici di studenti e docenti vengono rimossi al termine della permanenza nell'istituto (e con essi,tutti i contenuti prodotti dagli utenti).

Un mese prima della disattivazione, gli studenti ricevono via email l'avviso di disattivazione e le istruzioni per trasferire - se lo desiderano - i contenuti prodotti su altro account personale.

Strumenti di comunicazione online che possono essere utilizzati in ambito scolastico:

COMUNICAZIONE ESTERNA: strumenti utilizzati dalla scuola, sia per raggiungere target esterni, al fine di valorizzare e promuovere le attività portate avanti dall’Istituto, sia per far circolare all’interno della scuola informazioni di servizio o

contenuti importanti fra i diversi attori scolastici: sito web della scuola, profili sui social network (Facebook). Hanno lo scopo di trasmettere all'esterno l'identità, i valori, le azioni, i progetti e l'idea di educazione che l'Istituto porta avanti. La comunicazione esterna dell'Istituto può essere progettata ed implementata anche con il supporto degli studenti che possono produrre contenuti multimediali da diffondere attraverso i vari canali in uso.

COMUNICAZIONE INTERNA: hanno lo scopo di facilitare e rendere più partecipata la didattica e la comunicazione a scuola: registro elettronico, email istituzionale, app di Google Workspace.

In riferimento all'uso degli strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne,è importante ricordare quello che si può definire **"diritto alla disconnessione"** (art. 30 - Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola del CCNL 2019/2021).
I docenti, salvo in caso di comprovata urgenza, possono essere contattati via email tra le 08:00 e le 18:00 dei giorni feriali. In ogni caso non sono tenuti a rispondere alle email ricevute al di fuori di tale orario.

Per le chat informali fra colleghi, o fra docenti e genitori, non esiste una vera e propria regolamentazione, e per tale ragione si stabiliscono le seguenti regole condivise sull'uso:
Mettere in chiaro fin dall'inizio, comprendere e rispettare sempre le finalità del gruppo, scrivendo e pubblicando solo contenuti pertinenti a tali finalità;
Usare sempre un linguaggio adeguato e il più possibile chiaro e preciso (come già sottolineato la comunicazione online si presta spesso a non pochi fraintendimenti);
Evitare di affrontare in chat argomenti troppo complessi e controversi (la comunicazione online in una chat di gruppo non è adatta per la gestione di problematiche di questo tipo, che certamente è più opportuno affrontare in presenza o in un Consiglio di classe);
Evitare discussioni di questioni che coinvolgono due o pochi interlocutori, onde evitare di annoiare e disturbare gli altri componenti del gruppo;
Non condividere file multimediali troppo pesanti;
Evitare il più possibile di condividere foto di studenti in chat;
Indirizzare solo domande precise e chiare, a cui si possano dare risposte altrettanto brevi e precise;
Evitare messaggi troppo spezzettati, cercando il più possibile di essere brevi ed esaustivi allo stesso tempo.

Il **registro elettronico** permette di gestire la comunicazione con le famiglie, le quali attraverso di esso possono visualizzare molte informazioni utili, interagendo con la scuola, su: andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari); risultati scolastici (voti, documenti di valutazione); udienze (prenotazioni colloqui individuali); eventi (agenda eventi); circolari e comunicazione varie (comunicazioni di classe, comunicazioni personali).

Per quanto riguarda i compiti per casa, il registro elettronico non sostituisce in alcun modo il **diario scolastico**, come da normativa recentemente aggiornata. L'obiettivo è responsabilizzare gli studenti nello sviluppo di autonomia, organizzazione e abilità di scrittura.

- 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 chetrattitaliaspetti,considerandoaspettipositiviedeventualicriticitànellaeperladidattica.

L'istituto incoraggia il BYOD. L'uso dei device personali degli studenti è regolamentato dal Regolamento di istituto. Lo studente è responsabile del proprio devide personale come di ogni altro personale materiale scolastico.

Cap 4 – Segnalazione e gestione dei casi

- 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.

- 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 e cyberbulismo (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 sia la vittima 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 digrave difficoltà e va intesa come un momento di condivisione e solidarietà nei confronti del minore. La mancatasegnalazionecostituisce,infatti,omissionediattid'ufficio(art.328C.P.).

Può essere utile, valutando accuratamente ciascuna situazione, attivare colloqui individuali con tutti i minori coinvolti, siano essivittime,testimonie/oautori.Èimportanteconsiderareilpossibilecoinvolgimentodeigenitoriedicoloroincaricatidella 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 definiscel'istituto(mailadhoc,tramitegliufficiepostazionispecifiche,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

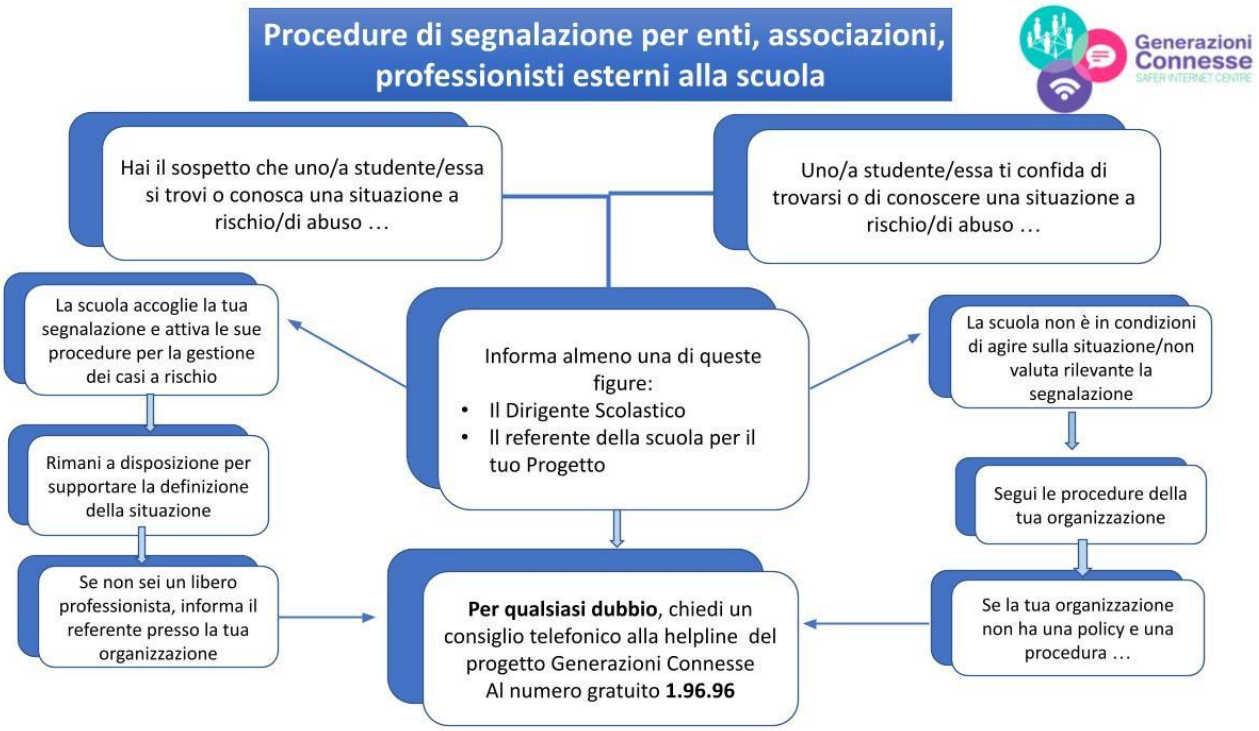
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta 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 DDI 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.

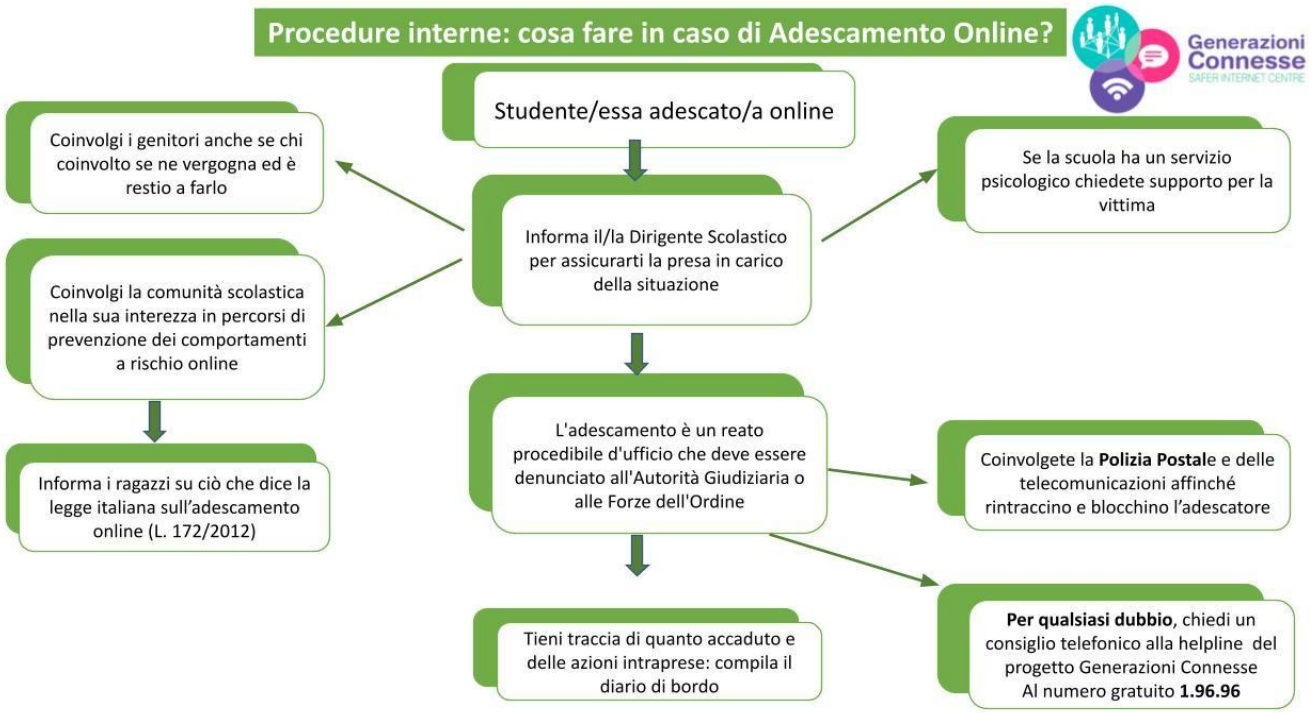
Se emergono evidenze passa allo schema successivo

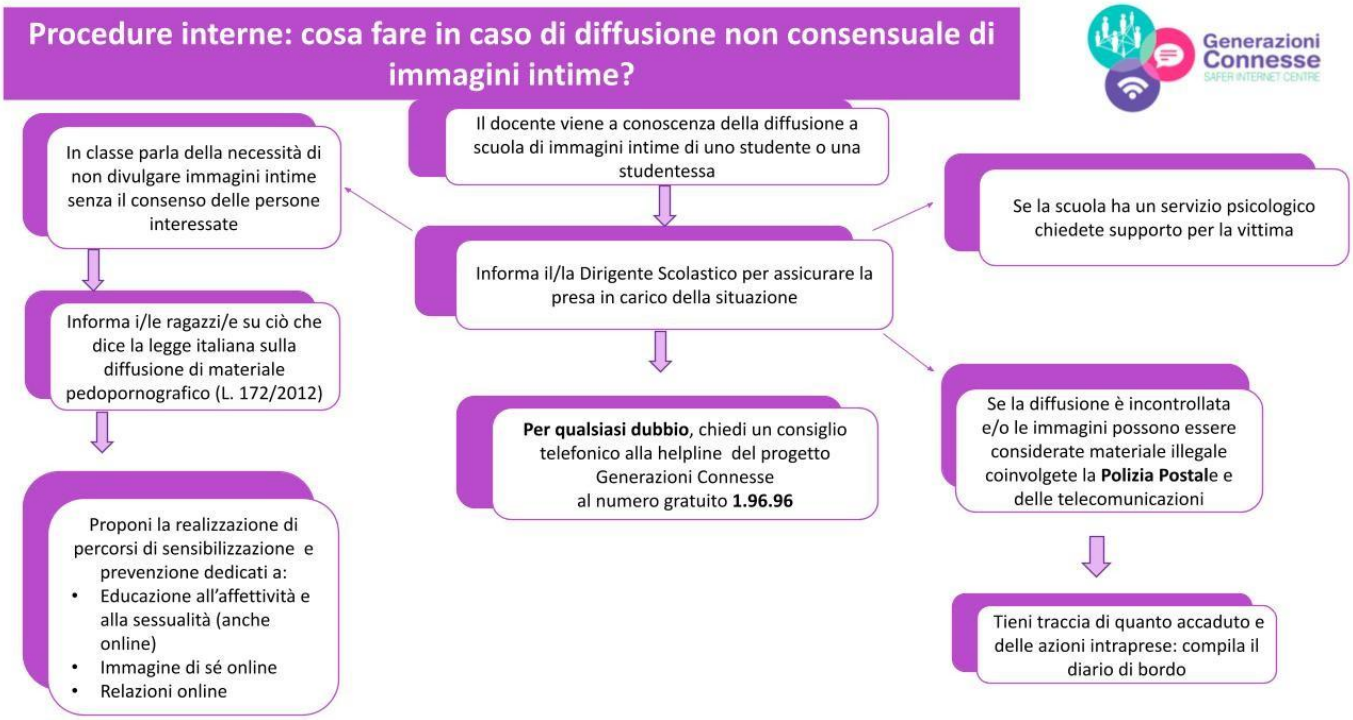
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

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





Per raccogliere le segnalazioni degli studenti e fornire loro informazioni e supporto, la scuola ha attivato l'indirizzo email sosbullismo@taddeocossu.edu.it.

È inoltre presente a scuola uno sportello d'ascolto affidato a un professionista esterno a cui è possibile rivolgersi previo appuntamento.

Allegato: Reati procedibili d'ufficio