



ISTITUTO D'ISTRUZIONE SUPERIORE

"GIANCARLO SIANI"

Via S. Gatto n. 24/A – 80131 – Napoli

Sede Succursale – Corso Chiaiano n. 50 – Napoli Dist.

Scol. N.43 Cod. Fisc. 95170160634

Cod. Min. NAIS099003 Tel. 081.545.62.14



I.I.S. "G. SIANI" - NAPOLI

Prot. 0009011 del 16/09/2025

IV (Uscita)

DOCUMENTO di ePOLICY

Delibera n. 32 del CdD del 08/09/2025

Delibera n. 11 del CdI del 09/09/2025



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 – Il Rischio on line

1. Sensibilizzazione e prevenzione
2. La formazione
3. Il curriculum digitale
4. 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. L'accesso ad internet
3. Strumenti di comunicazione online
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
4. Strumenti a disposizione di studenti e studentesse

Allegati con le procedure

Cap 1 - Presentazione della ePolicy

1.1 Scopo dell'ePolicy

La pervasività del digitale nella società attuale è un dato incontrovertibile e, come dimostra l'esplosione dell'Intelligenza Artificiale (AI), l'utilizzo delle tecnologie informatiche non solo è inarrestabile ma è in fase di sviluppo esponenziale.

La dotazione di strumentazione informatica a disposizione della scuola si è ampiamente arricchita, rendendo la regolamentazione delle TIC ancora più urgente.



Attraverso l'ePolicy, l'I.I.S. "Giancarlo Siani" di Napoli, intende dotarsi di uno strumento programmatico a cui l'intera comunità educante potrà fare riferimento **per promuovere un uso positivo delle nuove tecnologie al fine di riconoscere, prevenire e rispondere a possibili situazioni problematiche** e tradurre in modalità operative condivise i suggerimenti contenuti nella normativa di riferimento.

L'obiettivo è quello di garantire ai nostri studenti un **benessere digitale** attraverso la **sensibilizzazione**, l'**educazione**, l'**informazione**, la **formazione** con il coinvolgimento di docenti e famiglie. Ciò al fine della promozione di una cittadinanza digitale attiva che prevede **senso di responsabilità, diritti** ma anche **Doveri e regole da conoscere e da rispettare** per favorire un approccio consapevole, critico, in grado di valutare le opportunità offerte dalla rete e dal digitale e i rischi connessi.

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.

Adottare un **approccio preventivo** consente di individuare e affrontare i problemi ancor prima che si manifestino, contrastando la formazione di situazioni che minacciano il benessere dell'intera comunità scolastica. Questa strategia permette inoltre di ottimizzare l'uso delle risorse, evitando di affrontare le manifestazioni del problema in fasi più avanzate, quando l'intervento diventa più difficile e complesso.

1.2 - Ruoli e responsabilità nell'implementazione dell'ePolicy

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, si impegni nell'attuazione e promozione di essa.

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 DS che è 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 alle 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.

Infine, ha il compito di Intervenire (come gruppo ristretto, composto da Dirigente e referente o referenti per il bullismo e il cyberbullismo e psicologo, se presente) nelle situazioni acute di bullismo.

I/LE DOCENTI



ISTITUTO D'ISTRUZIONE SUPERIORE

"GIANCARLO SIANI"

Via S. Gatto n. 24/A – 80131 – Napoli

Sede Succursale – Corso Chiaiano n. 50 – Napoli Dist.

Scol. N.43 Cod. Fisc. 95170160634

Cod. Min. NAIS099003 Tel. 081.545.62.14



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.

Essi devono accompagnare e supportare gli/le studenti/esse 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 risultare poco opportuni 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 gli studenti uno strumento di ricerca e una fonte 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 qualunque problematica, violazione o abuso, anche online, che veda coinvolti gli studenti e 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 e/o cyberbullismo.

GLI STUDENTI E LE STUDENTESSE

Gli studenti 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 di classe e di Istituto degli studenti sono tenuti a diffondere i contenuti del documento di ePolicy e sono invitati a creare momenti di riflessione durante periodi di cogestione studentesca (es. settimana dello studente, attività per l'open day, ecc.)

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 - e 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 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.

Tutti coloro che entrano in contatto con gli studenti del nostro Istituto e che creano una relazione educativa con loro, sia nello svolgimento della prassi didattica ordinaria che nell'attuazione di progetti di ampliamento dell'offerta formativa in qualità di esperti esterni, sono tenuti a:

- conoscere l'e-Policy di Istituto
- mantenere un alto profilo personale e professionale
- evitare atteggiamenti inappropriati
- essere guidati dal principio dell'interesse superiore del minore

Tutti gli attori esterni devono conoscere e rispettare le regole del nostro Istituto in termini di:

- Utilizzo dei dispositivi (smartphone, tablet, PC...) personali e in dotazione della scuola.
- Rispettare la privacy, soprattutto dei minorenni, in termini di video, foto, contatti personali come numero telefono privato, chat di gruppo, e-mail, profili social.

Gli esperti esterni sono chiamati a osservare le regole e assicurarsi che vengano rispettate e sono tenuti a segnalare secondo le procedure indicate eventuali casi di uso improprio delle tecnologie digitali.

1.3 Integrazione ePolicy nei documenti scolastici e normativa generale

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

- **Regolamento dell'Istituto scolastico**, che rappresenta il principale punto di riferimento normativo e richiama le norme comportamentali.



- **Regolamento sull'uso dei dispositivi digitali a scuola** che definisce le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione in ambiente scolastico, in ottemperanza alla normativa vigente.
- **Patto di Corresponsabilità educativa** tra scuola e famiglia, 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 (PTOF) con relativo Rapporto di Autovalutazione (RAV) e Piano di miglioramento (PDM)**, 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 educative legate al percorso di ePolicy.

1.4 Condivisione e comunicazione dell'ePolicy all'intera comunità educante

Il documento di E-Policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli studenti) si faccia a sua volta promotore del documento.

L'E-Policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola (nella sezione Regolamenti);
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

2. 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 civica cittadinanza** mentre la versione per le famiglie è condivisa nel corso dei colloqui scuola-famiglia.

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).

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 Comune (servizi istruzione e servizi sociali) attraverso gli allegati sintetici progettati che indicano gli elementi del documento e le prospettive per la comunità.

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);

Piano d'azione triennale

- 1) rilevazione dei bisogni e grado di conoscenza del fenomeno da parte di famiglie, studenti e docenti per comprendere quali sono le necessità della comunità scolastica;
- 2) rilevazione di interessi, bisogni e comportamenti delle famiglie sull'uso positivo del digitale.
- 3) integrazione dal punto di vista amministrativo del documento dell'ePolicy all'interno degli altri documenti della scuola;
- 4) realizzazione di un momento informativo per la presentazione dell'ePolicy al corpo docenti in seno al Collegio dei docenti di inizio anno.
- 5) realizzazione di un momento informativo con le famiglie anche on line;
- 6) Sportello di ascolto psicologico per studenti.
- 7) Progetto accoglienza nella prima settimana di scuola per promuovere la socializzazione e condividere le regole della comunità scolastica;



- 8) Progetti di educazione all'affettività -e mozioni.
- 9) diffusione dell'ePolicy all'interno degli ambienti scolastici tramite:
 - apposita sezione del sito istituzionale
 - apposite circolari sul registro elettronico
 - pannelli all'interno dell'edificio scolastico (corridoi, aule...)
 - pagine social della scuola
- 10) formazione di docenti, studenti e famiglie a partire dalle classi prime anche grazie alla collaborazione di apposite associazioni (es. Associazioni di promozione sociale, Asl di riferimento territoriale; Generazioniconnesse, #cuoricone, Polizia Postale...);
- 11) promuovere contest/ concorsi, assemblee di istituto, focus tematici durante la settimana degli studenti ed altre attività rivolte agli studenti al fine di aumentare il grado di sensibilizzazione ed engagement;
- 12) armonizzazione nel curriculum integrato di Istituto di educazione civica, dei temi educazione civica digitale, bullismo e cyberbullismo;
- 13) calendarizzazione di incontri periodici del team antibullismo e cyberbullismo per monitoraggio e valutazione;
- 14) messa a disposizione della comunità educante di un modulo di prima segnalazione (per chiunque abbia necessità di segnalare situazioni a rischio di presunto o reale bullismo/cyberbullismo;
- 15) aggiornamento continuo tramite i canali istituzionali e social dell'Istituto.

Cap 2 – Il Rischio on line

2.1 - Sensibilizzazione e prevenzione

Il rischio online si configura come la possibilità per il minore di:

- commettere azioni online che possano danneggiare se stessi o altri;
- essere una vittima di queste azioni;
- osservare altri commettere queste azioni.

È importante riconoscere questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per arginarli e contenerli, ma è altrettanto importante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano. Ciò è possibile lavorando su aspetti di ampio raggio che possano permettere una riduzione dei fattori di rischio e di conseguenza una minore probabilità che i ragazzi si trovino in situazioni non piacevoli. È importante che abbiano gli strumenti idonei per riconoscere possibili situazioni di rischio e segnalarle ad un adulto di riferimento.

Gli strumenti da adottare per poter ridurre l'incidenza di situazioni di rischio si configurano come



interventi di sensibilizzazione e prevenzione.

-Nel caso della sensibilizzazione si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere e riconoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.

-Nel caso della prevenzione si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di ragazze/i.

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.

2.2- La Formazione

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

La competenza digitale, oggi, è imprescindibile per i docenti così come per studenti e studentesse e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa e in grado di venire incontro ai nuovi stili di apprendimento.

Pertanto l'Istituto riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola, dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dai docenti (anche online) sulle TIC e si impegna a organizzare ogni anno momenti di formazione sui metodi e sugli strumenti della didattica digitale.

La formazione di studenti e famiglie avverrà, come già da molti anni, a partire dalle classi prime, dedicando particolare attenzione al primo biennio, anche grazie alla collaborazione di apposite associazioni ed enti (es.ASL, Generazioniconnesse, #cuoriconnessi, Polizia Postale...).

Si terrà conto, della Giornata Mondiale dedicata alle tematiche del cyberbullismo e della sicurezza in rete (*Safer Internet day*, 11 febbraio) e della Giornata del rispetto e delle vittime del bullismo (20 gennaio) istituita dalla legge 70/2024 .

Agli studenti del triennio verrà proposta la formazione on line sulla piattaforma Generazioni Connesse.

2.3 - Il Curricolo Digitale



Nel Quadro comune di riferimento europeo per le competenze digitali (Digcomp 2.2) nonché nell'ambito degli orientamenti normativi scolastici (Indicazioni Nazionali 2012; Piano Nazionale Scuola Digitale 2015; Linee guida per la certificazione delle competenze 2017), il curricolo digitale è definito come un percorso didattico verticale pensato per tutti gli studenti e le studentesse teso a sviluppare, e poi potenziare, le cosiddette "competenze digitali" in ottica trasversale (su più livelli, anni e gradi di istruzione) ed interdisciplinare (per tutte le discipline). Si tratta, quindi, di **favorire la capacità dell'uso dei dispositivi digitali non solo da un punto di vista strettamente tecnico, ma anche e soprattutto da un punto di vista etico, responsabile e critico (pensiero critico) utile allo sviluppo della cittadinanza digitale** tramite la progettazione e la sperimentazione di percorsi, attività e laboratori in aula dedicate al digitale tra opportunità, rischi e sfide del prossimo futuro. Il Curricolo Digitale ha lo scopo di programmare ed implementare percorsi didattici di facile replicabilità, uso e applicazione che siano "innovativi, strutturati, aperti e in grado di coinvolgere la comunità scolastica allargata" sul tema del digitale e delle tecnologie digitali. In questo modo, si può rendere quanto più possibile integrato e consapevole l'utilizzo dei dispositivi digitali, così come anche esplicitato nel DigComp Edu (quadro di riferimento europeo sviluppato dalla Commissione Europea che definisce le competenze digitali essenziali che ogni cittadino deve possedere) secondo cui lo sviluppo delle competenze digitali degli studenti contribuisce ad *aiutarli ad utilizzare in modo creativo e responsabile le tecnologie digitali, per attività riguardanti l'informazione, la comunicazione, la creazione di contenuti, il benessere personale e la risoluzione dei problemi.*

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

3.1 Protezione dei dati personali

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 UE 2016/679 noto anche come GDPR
- il D.lgs. 196/2003 conosciuto come Codice Privacy, Codice in materia di protezione dei dati personali, vigente in Italia, prima dell'approvazione del regolamento europeo UE 2016/679 e, successivamente novellato dal D.lgs. 101/2018, per l'adeguamento alle norme europee.

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 obbligatoriamente designare di provvedere alla designazione di un Responsabile della protezione dei dati personali (RPD o DPO).

L'RPD deve avere particolari qualità professionali e un'approfondita conoscenza della normativa in



materia di dati personali.

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;

-nella tenuta di un documento di sintesi, in cui sono riportate tutte le informazioni sui trattamenti effettuati e sulle categorie di dati utilizzati. La scuola non è tenuta a richiedere il consenso laddove il trattamento dei dati personali viene effettuato per perseguire delle finalità di natura istituzionale, in quanto previsto dalla legge. Tuttavia, il consenso privacy diventa necessario laddove la scuola intenda effettuare un trattamento di dati personali finalizzato ad attività che non rientrano tra quelle istituzionali o didattiche, come ad esempio l’organizzazione di corsi di musica, di corsi teatrali o comunque attività che non rientrano in quello che è il curriculum scolastico;

-nella predisposizione di una procedura per la violazione dei dati che consenta alla scuola di reagire prontamente in caso di violazione dei dati personali, ad esempio attacco informatico. Inoltre vanno indicati i tempi di conservazione dei dati e le misure di sicurezza organizzative ed informatiche per la protezione dei dati.

3.2-L’Accesso ad internet

1. *L’accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
4. *L’accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

Così recita l’art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le “*misure riguardanti l’accesso a un’Internet aperto e che modifica la direttiva 2002/22/CE, relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all’interno dell’Unione*”.

Il diritto di accesso a Internet è dunque presente nell’ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di *fornire a tutte le scuole le condizioni per l’accesso alla società dell’informazione e fare in modo che il “diritto a Internet” diventi una realtà, a partire dalla*



scuola.

Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

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 della 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.

• **Utilizzo dei dispositivi informatici in dotazione all'istituto**

L'utilizzo dei device deve avvenire in maniera responsabile ed avendo cura sia degli apparati fisici, che dell'integrità dei software in essi installati. Sulla base di tali presupposti e per motivi di sicurezza, agli utenti è vietato:

- utilizzare i dispositivi per finalità personali o comunque non correlati con attività didattiche o di studio;
- collegare dispositivi esterni (memorie USB, hard disk, ecc.);
- installare e disinstallare i programmi o modificarne le impostazioni;
- copiare, caricare o scaricare musica, film, programmi e qualsiasi altro materiale non legato alla didattica o vincolato da copyright o comunque in conflitto con le norme dei codici civile e penale riguardanti il diritto d'autore, la privacy, la divulgazione di materiale offensivo, pedo-pornografico etc.

• **Accesso al Wi-Fi**

-Nel caso in cui i dispositivi in dotazione all'istituto abbiano accesso alla rete WiFi, sarà necessario dotarli di credenziali per l'accesso alla rete. Tali credenziali devono essere gestite con la massima cautela e riservatezza.

• **Utilizzo degli strumenti di didattica digitale**

L'accesso alle piattaforme didattiche dell'istituto deve essere consentito esclusivamente previa autenticazione informatica. A ciascun utente devono essere fornite credenziali univoche, che devono essere custodite con la dovuta diligenza.

• **Registro elettronico**

L'accesso al registro elettronico viene abilitato per docenti, genitori e studenti tramite credenziali di accesso da custodire con la dovuta diligenza. Il registro elettronico deve essere utilizzato esclusivamente per le finalità istituzionali predeterminate dall'istituto (es. Caricamento e lettura voti, assenze, avvisi, ecc.)



● Responsabilità

Durante l'accesso ad internet nei laboratori informatici, o in aula su consenso dei docenti e sotto la loro vigilanza, **gli alunni 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 senza autorizzazione;
- tenere spento lo smartphone durante le attività scolastiche** che non ne prevedano l'utilizzo specifico a fini didattici (a meno che non siano autorizzati in deroga a quanto sancito nel *Regolamento sull'uso dei dispositivi digitali a scuola*);
- durante le attività che prevedono l'utilizzo dello smartphone utilizzarlo in modo adeguato a quanto previsto;
- segnalare immediatamente situazioni inadeguate ai docenti;

I docenti si impegnano a:

- utilizzare la rete in 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 che prevedono l'uso di device;
- monitorare l'uso che gli studenti fanno delle tecnologie a scuola.

3.2 Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

Strumenti di comunicazione online che possono essere utilizzati a scuola:

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, Bacheca Argo Famiglia. 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 ARGO, Suite di strumenti GOOGLE



Il Registro Elettronico -ARGO

Tutti i docenti e gli alunni hanno a disposizione un account personale grazie al quale possono usare i servizi della Suite di Google.

Le comunicazioni relative a valutazioni, circolari, autorizzazioni, provvedimenti disciplinari ecc. vengono veicolati attraverso la piattaforma Argo sezione Bacheca. Le programmazioni, i piani di lavoro individuali, le relazioni finali ecc. vengono pubblicate nella sezione "Condivisione Documenti". Sono pubblicati sul sito della scuola, documenti e contenuti comunicativi rivolti agli utenti esterni. Inoltre i docenti possono anche condividere con gli alunni contenuti didattici in formato digitale secondo modalità concordate e nel rispetto delle norme vigenti.

SUITE di GOOGLE

Gli studenti, i docenti ed i genitori prendono atto, alla luce della presente informativa, che i servizi offerti sono ESCLUSIVAMENTE per utilizzo scolastico e didattico.

In riferimento all'uso degli strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne, come avviene generalmente fra i docenti mediante, ad esempio, l'uso di gruppi WhatsApp, è importante ricordare quello che si può definire "diritto alla disconnessione" (art. 22 - Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola del CCNL 2016/2018).

Per le chat informali fra colleghi, o fra docenti e genitori Rappresentanti di classe (o in via eccezionale con genitori di studenti con particolari e comprovate problematiche) 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 personali, complessi o 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 disturbare gli altri componenti del gruppo;

sempre nell'ottica che, anche se nessuna legge vieta espressamente WhatsApp tra docenti, il Garante della Privacy e diverse Linee guida ministeriali (MIUR/MI) raccomandano prudenza nell'uso di questa che non è una piattaforma istituzionale e quindi priva di valore legale. L'uso deve essere comunque limitato a comunicazioni non sensibili e a carattere organizzativo immediato.

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;
- violare 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.

Per il momento la scuola non si è dotata di questo documento.

4.3 Strumentazione personale (BYOD)

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/le studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo e il più ampio PNSD.

La presente ePolicy contiene 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 MIM per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica che, alla luce della recente normativa (Circolare MIM del 16/06/2025), è stata regolamentata nel *Regolamento di Istituto sull'uso dei dispositivi digitali a scuola*, recante norme per l'utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica.

Da tale documento si evince che pur quando l'uso del device è autorizzato dal docente, **il discente ha il dovere:**

- di assolvere assiduamente agli impegni di studio e durante gli orari di lezione;
- **di tenere comportamenti rispettosi degli altri, nonché corretti e coerenti con i principi del diritto alla privacy. In virtù della normativa vigente (C.M. 16/06/2025 nota prot. 3392), è fatto divieto di utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire, divulgare e/o pubblicare immagini, filmati o registrazioni vocali. In altre parole, è punibile sia a livello civile che penale (oltre che le sanzioni previste dagli artt. 3 e 4, d.P.R. 24 giugno 1998, n. 249 - "Regolamento recante lo statuto delle studentesse e degli studenti della scuola secondaria"), chi abusa dei dati personali altrui raccolti (immagini, filmati, registrazioni vocali...), violandone la privacy.;**

I genitori: sono tenuti ad osservare le disposizioni organizzative dettate dal Regolamento di Istituto che richiama ai loro doveri di vigilanza e di corresponsabilità e invita, pertanto, le famiglie degli studenti ad impegnarsi a rispondere direttamente dell'operato dei propri figli nel caso in



cui, ad esempio, gli stessi arrechino danni ad altre persone o, più in generale, violino i doveri sanciti dal Regolamento di Istituto e subiscano, di conseguenza, l'applicazione di una sanzione disciplinare.

Il Dirigente, i docenti e il personale ATA: hanno il dovere di vigilare sui comportamenti degli studenti e delle studentesse e di segnalare eventuali infrazioni suscettibili di sanzioni disciplinari.

Cap 4 - Segnalazione e gestione dei casi

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. 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. (Vedi *REGOLAMENTO PER LA PREVENZIONE E CONTRASTO AL BULLISMO E AL CYBERBULLISMO. PROTOCOLLO* (Legge 70/2024 art.4 comma 2bis))
Nelle procedure sono indicate:

- **le figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso;**
- **le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.** 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 si prevede la collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio, qualora la gravità 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 potrà avvenire 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 il sito della scuola, durante i collegi docenti, attraverso tutti i canali maggiormente utili ad un'efficace comunicazione (Bachecca Argo famiglia).

4.1 Cosa segnalare

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. È necessario poi valutare l'eventuale stato di disagio vissuto dagli/le 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 all'adolescente, evitando, quindi, di rispondere



all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. 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 rivolgersi immediatamente alla Polizia Postale

4.2 Come segnalare: Quali strumenti e a chi

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, o alla Polizia Postale che rimuoverà i contenuti entro 48 ore.

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, 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 coordinatore di classe,
3. L'animatore 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.

Sulle procedure della segnalazione vedi *REGOLAMENTO PER LA PREVENZIONE E CONTRASTO AL BULLISMO E AL CYBERBULLISMO. PROTOCOLLO* (Legge 70/2024 art.4 comma 2bis)



4.3 Gli attori sul territorio

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

Talvolta, nella gestione dei casi, il Dirigente Scolastico, oltre alle famiglie, può **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale:** supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni:** accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali:** forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico:** segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danni dovuti a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori

4.4 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 prevede alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni che consente di avviare la procedura
- sportello di ascolto;
- docente referente per bullismo e cyberbullismo
- docenti.