

I.T.E.T. "G. SALVEMINI" - MOLFETTA
Prot. 0007464 del 26/06/2025
I (Uscita)

Documento di ePolicy

ISTITUTO TECNICO "GAETANO SALVEMINI"

VIA TEN. ANGELO LUSITO 94 - 70056 - MOLFETTA
Bari (BA) - Puglia

Data di approvazione: 26/06/2025

Indice

Capitolo 1 - Presentazione del documento 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

- 2.1. Sensibilizzazione
- 2.2. Il Curriculo digitale
- 2.3. Il Kit Didattico

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

- 3.1. Protezione dei dati personali e GDPR
- 3.2. Accesso ad Internet
- 3.3. Strumenti di comunicazione online (PUA)

Capitolo 4 - Segnalazione e gestione dei casi

- 4.1. Cosa segnalare
- 4.2. Come segnalare: quali strumenti e a chi
- 4.3. Gli attori sul territorio per intervenire
- 4.4. Allegati con le procedure

Allegati

1.1 Scopo dell'ePolicy

Negli ultimi anni le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento nelle scuole. La competenza digitale inoltre, è una competenza chiave del cittadino europeo all'interno del "Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente" e in base alle Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018.

La scuola quindi, deve avere come obiettivo la formazione di cittadini digitali competenti, responsabili e rispettosi delle regole della convivenza online. Alla luce di quanto evidenziato L'ITET Salvemini da più di un decennio ha notevolmente incrementato l'uso dei dispositivi e di tutte le tecnologie digitali per promuovere metodologie didattiche più accattivanti ed in linea con i tempi.

L'E-policy è quindi necessaria per fornire delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC nel contesto scolastico, ponendo le basi per azioni formative e educative sulle tecnologie digitali.

Nello specifico lo scopo dell'ePolicy dell'Istituto Tecnico Economico e Tecnologico "G. Salvemini" è quello di promuovere un uso sicuro, consapevole e responsabile delle tecnologie digitali all'interno della comunità scolastica. Essa si inserisce nel quadro delle azioni di cittadinanza digitale previste nel Piano Triennale dell'Offerta Formativa (PTOF) dell'istituto seguendo le linee guida del progetto ministeriale ispirandosi alle linee e agli obiettivi delineati nel progetto nazionale di "Generazioni Connesse" (Safer Internet Centre).

Obiettivi principali dell'ePolicy

Nello specifico il documento autoprodotto dalla scuola ha individuato i seguenti principali obiettivi:

- Promozione delle competenze digitali:** Fornire agli studenti e al personale scolastico gli strumenti necessari per sviluppare competenze digitali avanzate, essenziali per affrontare le sfide del mondo contemporaneo e per favorire l'inclusione digitale.
- Sicurezza online:** Implementare misure preventive e strategie di intervento per affrontare problematiche legate all'uso improprio delle tecnologie digitali, come il cyberbullismo, l'hate speech e altre forme di abuso online.
- Integrazione delle TIC nella didattica:** Incoraggiare l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC) come strumenti didattici, migliorando l'efficacia dell'insegnamento e l'apprendimento degli studenti.
- Coinvolgimento della comunità scolastica:** Favorire la partecipazione attiva di studenti, docenti, genitori e personale scolastico nella definizione e nell'attuazione delle politiche digitali dell'istituto, promuovendo una cultura condivisa della cittadinanza digitale.
- Allineamento con il PTOF:** Assicurare che le iniziative digitali siano coerenti con la missione educativa dell'istituto, che include l'internazionalizzazione, l'inclusione sociale e il potenziamento delle competenze trasversali degli studenti.

Implementazione dell'ePolicy

L'ePolicy è stata sviluppata attraverso un processo partecipativo che coinvolge un gruppo di lavoro composto da docenti rappresentanti dei vari indirizzi di studio dell'istituto, il dirigente scolastico, l'animatore digitale, il team digitale e i referenti rispettivamente della privacy e cyberbullismo. Questo

gruppo è responsabile della personalizzazione e redazione del documento, adattandolo alle specifiche esigenze e caratteristiche dell'ITET "G. Salvemini".

Il processo di elaborazione dell'ePolicy prevede le seguenti fasi:

- **Autovalutazione:** Analisi delle pratiche attuali relative all'uso delle tecnologie digitali e identificazione delle aree di miglioramento.
- **Formazione:** Partecipazione a corsi di formazione online offerti da "Generazioni Connesse" per acquisire le competenze necessarie alla redazione dell'ePolicy.
- **Redazione del documento:** Stesura dell'ePolicy, suddivisa in una parte standard comune a tutte le scuole e una parte personalizzata che riflette le specificità dell'istituto.
- **Implementazione e monitoraggio:** Attuazione delle misure previste dall'ePolicy e monitoraggio continuo per valutarne l'efficacia e apportare eventuali modifiche.

Attraverso l'elaborazione e l'implementazione dell'ePolicy, l'ITET "G. Salvemini" si impegna a creare un ambiente scolastico sicuro e inclusivo, dove le tecnologie digitali siano utilizzate in modo etico e consapevole, contribuendo alla formazione di cittadini digitali responsabili.

1.2 Ruoli e responsabilità nell'implementazione dell'ePolicy

L'attuazione dell'ePolicy coinvolge l'intera comunità scolastica. Nel presente documento, vengono definiti con chiarezza ruoli, compiti e responsabilità di ciascuna delle figure all'interno dell'Istituto.

- Il Dirigente Scolastico: supervisiona l'intero processo e ne garantisce l'attuazione;
- Il Referente eSafety: coordina il gruppo di lavoro e cura la formazione e la sensibilizzazione del personale;
- L'animatore digitale: promuove la cultura del digitale;
- Il Team Digitale: collabora alla gestione delle infrastrutture e alla diffusione delle buone pratiche;
- I Docenti: integrano i principi dell'ePolicy nella didattica quotidiana;
- Gli Alunni e le Famiglie sono i destinatari e i promotori di comportamenti responsabili nell'uso delle tecnologie.

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.

Qui di seguito evidenziamo nei dettagli tutti i compiti e le responsabilità delle su indicate figure professionali che si occupano di gestione e programmazione delle attività formative, didattiche ed educative dell'Istituto e tutte quelle figure appartenenti alla comunità educante che hanno compiti e responsabilità specifiche che qui di seguito evidenziamo.

IL DIRIGENTE SCOLASTICO: la prof.ssa Pasqualina Pierro

Il Dirigente Scolastico nel promuovere l'uso consentito delle tecnologie digitali, promuovere la cultura della sicurezza online e per tutti i membri della comunità scolastica, in linea con il quadro normativo di

riferimento, le indicazioni del Ministero della Pubblica istruzione e del merito e delle sue agenzie, mantenendosi costantemente aggiornato attraverso corsi di formazione promossi dalle istituzioni scolastiche al fine di garantire una cultura digitale consapevole. Presiede il Team per la prevenzione e il contrasto del bullismo e del cyberbullismo, collabora con i docenti referenti e gestisce direttamente, insieme ai Consigli di classe, i casi più gravi di comportamenti scorretti e uso improprio delle tecnologie. Attraverso queste azioni, il Dirigente Scolastico assicura un ambiente scolastico sicuro, inclusivo e attento al benessere di tutti. In particolare:

- **Definisce le linee guida** del PTOF e del Patto di Corresponsabilità (D.P.R. 235/07), integrando misure specifiche di prevenzione;
- **Aggiorna il Regolamento d'Istituto e di disciplina**, con regole condivise per il contrasto dei fenomeni di bullismo e cyberbullismo;
- **Informa costantemente le famiglie** sulle iniziative intraprese, anche tramite il sito web della scuola e il portale;
- **Organizza e coordina attività educative** e corsi di aggiornamento per studenti, genitori, personale docente e non docente, coinvolgendo esperti e collaborando con enti locali, associazioni, istituzioni e altre scuole;
- **Promuove un uso sicuro e responsabile di Internet**, garantendo sia gli aspetti tecnologici che quelli psicopedagogici;
- **Stipula accordi con i servizi territoriali** (sanitari, sociali, forze dell'ordine, giustizia minorile) per offrire supporto continuativo agli studenti coinvolti;
- **Nomina uno o più referenti scolastici** per la prevenzione del bullismo e cyberbullismo, su proposta del Collegio dei Docenti.

L'ANIMATORE DIGITALE Prof.ssa Rosa Andriani e IL TEAM PER L'INNOVAZIONE DIGITALE, Prof.ssa V. Altomare, prof.ssa R. Campi, prof. M. Ciccolella, Prof. D. Fasciano, prof. S. Patimo.

L'Animatore Digitale è una figura chiave per l'attuazione del Piano Nazionale Scuola Digitale e riveste un ruolo strategico nel promuovere una cultura digitale responsabile e sicura all'interno dell'Istituto. Il suo compito non si limita al solo supporto tecnico-informatico, ma si estende anche all'ambito della **prevenzione dei rischi online**, della **protezione dei dati personali** e dell'**uso consapevole delle tecnologie e della formazione** del personale scolastico. Nell'Istituto a supporto dell'animatore digitale è stato istituito il team dell'innovazione digitale. Tutte queste figure insieme al referente ePolicy, sono corresponsabili dell'attuazione dei piani di azione finalizzati ad un corretto e funzionale uso del digitale.

In particolare, l'Animatore Digitale:

- **Supporta il personale scolastico** nell'utilizzo delle TIC, offrendo assistenza sia tecnica che formativa, con particolare attenzione alla sicurezza informatica, alla privacy e alla gestione corretta dei dati personali;
- **Promuove e coordina percorsi di formazione interna** per docenti, studenti e personale ATA, su temi legati alla transizione digitale, alla cittadinanza digitale e alla prevenzione dei fenomeni di bullismo e cyberbullismo;
- **Monitora l'utilizzo delle tecnologie a scuola**, rilevando eventuali criticità o usi impropri e segnalando al Dirigente Scolastico le situazioni a rischio;

- **Garantisce il corretto accesso alla rete d'Istituto**, verificando che gli utenti autorizzati si autentichino tramite credenziali personali per finalità didattiche e istituzionali, nel rispetto delle policy scolastiche;
- **Collabora attivamente con il Team per l'Innovazione Digitale**, contribuendo alla progettazione di interventi formativi e innovativi;
- **Partecipa, su richiesta del Dirigente Scolastico**, alle attività di prevenzione e contrasto dei fenomeni di bullismo e cyberbullismo, anche in sinergia con i referenti designati e il Team antibullismo.
- **Partecipa alla redazione del documento di ePolicy**

Tutte le sue azioni sono orientate a favorire una scuola inclusiva, sicura e al passo con le trasformazioni digitali, secondo le linee guida del *Safer Internet Centre* e le indicazioni ministeriali in materia di e-safety.

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO prof.ssa A. Squeo.

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 cyber bullismo. Le **funzioni e gli ambiti di intervento del referente sono stati individuati dall'ITET Salvemini**, in attuazione dell'art. 4 della Legge 71/2017, e, sono: coordinare le iniziative di prevenzione, sensibilizzare e contrastare i fenomeni di bullismo e cyber- bullismo. Questa figura svolge un ruolo strategico sia a livello scolastico che extrascolastico, promuovendo interventi educativi e formativi rivolti a studenti, docenti e famiglie, anche in collaborazione con realtà del territorio.

In particolare, questo referente:

- **Costituisce l'interfaccia operativa** tra la scuola e soggetti esterni come Forze dell'Ordine, servizi minorili, associazioni, centri giovanili, servizi sociali e sanitari;
- **Promuove azioni educative, progetti d'Istituto e corsi di formazione** sull'uso consapevole delle nuove tecnologie e sulle responsabilità legali legate ai comportamenti online;
- **Collabora con esperti esterni** per la realizzazione di percorsi di prevenzione personalizzati e contestualizzati;
- **Favorisce la creazione di reti scolastiche**, coordinando momenti formativi interistituzionali come seminari, giornate tematiche e il "Safer Internet Day";
- **Supporta il Dirigente Scolastico** nella revisione e aggiornamento di documenti strategici quali il PTOF, il Regolamento di Istituto, il PdM e il RAV;
- **Raccoglie e diffonde buone pratiche** e azioni di monitoraggio, contribuendo all'elaborazione e all'aggiornamento della ePolicy d'Istituto;
- **Partecipa a percorsi di formazione dedicati**, anche attraverso piattaforme ministeriali, per consolidare competenze specifiche nel contrasto ai fenomeni di bullismo e cyberbullismo.

Attraverso questi compiti, il referente del Cyberbullismo garantisce un presidio costante di prevenzione e accompagna la comunità scolastica nella costruzione di un ambiente educativo digitale sicuro, inclusivo e rispettoso.

I DOCENTI

Tutti i 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 studentesse e studenti nelle attività di apprendimento e nei laboratori che prevedono l'uso della DIGITAL BOARD 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 docenti osservano altresì regolarmente i comportamenti a rischio (sia dei potenziali bulli, sia delle potenziali vittime) e hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che veda coinvolti studenti e studentesse dandone tempestiva comunicazione al Dirigente Scolastico, al Referente per il Cyberbullismo e Bullismo e al Consiglio di Classe per definire strategie di intervento condivise.

RESPONSABILE DELLA PROTEZIONE DEI DATI LiquidLow s.r.l. (Referente esterno) – Prof. D. Fasciano Referente ePolicy(interno)

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. L'Istituto affida allLiquidLow s.r.l., la fornitura del servizio esterno di Responsabile della Protezione dei Dati (RPD o DPO), secondo i compiti espressamente previsti dall'art 39 del Regolamento UE 2016/679. Questa azienda fornisce: tutti i servizi di consulenza in materia di amministrazione digitale e privacy; un calendario operativo che prevede sia attività presso l'Istituto che attività di back office. Per una migliore gestione dell'attività l'azienda si interfaccia con il referente ePolicy interno individuato.

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

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

GLI STUDENTI

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 studenti sono informati del documento di ePolicy e invitati a costruire i piani di azione per divulgare lo stesso nell'istituto.

I GENITORI

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

Tutti gli **enti pubblici e privati, le organizzazioni del terzo settore, le associazioni e i professionisti esterni** che operano con il nostro Istituto nell'ambito di progetti educativi e formativi, devono attenersi ai principi e alle disposizioni contenute nell'**ePolicy di Istituto**, con particolare riferimento all'uso consapevole delle Tecnologie dell'Informazione e della Comunicazione (TIC) e alla sicurezza in rete. 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.

Tali soggetti si impegnano a:

- **Conformarsi alla politica scolastica sull'uso positivo, responsabile e sicuro delle tecnologie digitali** durante tutte le attività rivolte agli studenti;
- **Valutare la coerenza delle proprie proposte progettuali** con i criteri di qualità e le finalità formative dell'ePolicy, promuovendo comportamenti digitali sicuri e consapevoli;
- **Implementare misure preventive e protettive** per la tutela dei minori, garantendo la tempestiva individuazione e presa in carico di eventuali situazioni di rischio o disagio online;
- **Promuovere ambienti educativi sicuri**, improntati al rispetto reciproco, alla protezione dei dati personali e all'interesse superiore dello studente.

Chiunque entri in contatto diretto con gli studenti dell'Istituto, stabilendo una relazione educativa in qualità di **esperto, collaboratore o formatore esterno**, è tenuto a:

- Conoscere e rispettare l'**ePolicy dell'Istituto**;

- Mantenere un **profilo personale e professionale elevato**, evitando ogni atteggiamento inappropriato o ambiguo;
- Osservare le **regole interne sull'uso dei dispositivi digitali** (personali e in dotazione della scuola);
- Rispettare la **privacy degli studenti**, in particolare dei minorenni, evitando la raccolta e la diffusione non autorizzata di immagini, video, contatti personali (numero di telefono, e-mail, account social, chat di gruppo).

Inoltre, gli esperti e collaboratori esterni:

- Sono responsabili del **rispetto delle regole da parte degli studenti durante le attività digitali**;
- Devono **vigilare sull'utilizzo corretto delle tecnologie** e segnalare eventuali comportamenti impropri o rischiosi;
- Devono seguire le **procedure di segnalazione previste dall'Istituto**, utilizzando gli strumenti predisposti (es. scheda di segnalazione allegata all'ePolicy), indicando, quando possibile, i soggetti coinvolti, la natura del comportamento e le circostanze osservate.

Responsabilità degli attori esterni coinvolti in attività educative

Tutti coloro che entrano in relazione educativa con gli studenti e le studentesse – siano essi docenti, esperti esterni o rappresentanti di enti e associazioni – sono tenuti a mantenere un comportamento sempre professionale, rispettoso e responsabile, fondato sul principio del superiore interesse del minore.

È fatto espresso divieto di qualsiasi atteggiamento irrispettoso o lesivo della dignità, della privacy e dell'integrità fisica e psicologica degli studenti, nonché della tolleranza o partecipazione ad azioni illegali, rischiose o abusive.

I soggetti esterni devono:

- Conoscere e rispettare le norme interne dell'Istituto, in particolare quelle relative all'uso corretto e responsabile dei dispositivi digitali (personalni o scolastici);
- Astenersi da qualsiasi utilizzo improprio o non etico delle tecnologie durante le attività educative;
- Rispettare la privacy dei minori, evitando la raccolta e la diffusione di immagini, contatti personali o contenuti sensibili senza esplicito consenso;
- Segnalare tempestivamente al Dirigente scolastico o ai Referenti per bullismo e cyberbullismo ogni episodio problematico o illecito legato all'uso delle tecnologie;

Per garantire trasparenza e tutela, l'Istituto può:

- Richiedere la **presa visione formale dell'ePolicy** da parte di ogni soggetto esterno prima dell'avvio delle attività didattiche;
- Valutare l'opportunità di richiedere il **casellario giudiziale**, in particolare per escludere eventuali condanne per reati contro i minori;

L'adozione condivisa dell'ePolicy, comprensiva delle **procedure di segnalazione** e di gestione delle criticità, rafforza il rapporto fiduciario tra scuola e famiglia, tutela gli studenti da condotte scorrette e consente alla scuola di attivare tempestivamente le autorità competenti e i servizi del territorio.

1.3 Integrazione ePolicy nei documenti scolastici

La trasversalità dell'ePolicy rende necessaria una sua integrazione nell'ambito dei documenti che disciplinano il funzionamento dell'Istituto Scolastico a tal fine è stata attivata nei seguenti documenti in base a quanto specificato:

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.

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

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

1.4 Condivisione e comunicazione dell'ePolicy

Diffusione e condivisione dell'ePolicy d'Istituto

Il documento di **ePolicy** è uno strumento fondamentale per promuovere la cultura della sicurezza digitale e dell'uso consapevole delle tecnologie all'interno della scuola. Esso viene condiviso con l'intera comunità educante, ponendo al centro la tutela, il benessere e la crescita degli studenti e delle studentesse e definendo in modo chiaro ruoli, compiti e responsabilità di ciascun attore scolastico. È quindi essenziale che ogni componente della scuola: docenti, personale ATA, studenti, famiglie e collaboratori esterni, si riconosca nel documento e ne diventi promotore attivo, contribuendo alla diffusione di comportamenti responsabili nell'ambiente scolastico e digitale.

La condivisione dell'ePolicy avviene attraverso:

- La **pubblicazione sul sito web istituzionale** dell'Istituto, nell'area dedicata alla documentazione scolastica;
- L'inclusione dei principi fondamentali dell'ePolicy nel **Patto Educativo di Corresponsabilità**, sottoscritto da famiglie e studenti all'inizio di ogni anno scolastico;
- L'approvazione formale da parte del **Collegio dei Docenti** e del **Consiglio di Istituto**, che ne garantiscono la legittimità e l'adozione a livello istituzionale;
- La **diffusione del documento in formato semplificato** in tutti gli spazi scolastici dotati di dispositivi connessi alla rete (laboratori, aule multimediali, biblioteche, ecc.), nonché in punti strategici dell'edificio scolastico, al fine di garantirne la piena visibilità e accessibilità.

La promozione dell'ePolicy si inserisce in una più ampia strategia educativa che mira a coinvolgere l'intera comunità scolastica nella costruzione di un ambiente digitale sicuro, inclusivo e rispettoso, in coerenza con le finalità del Piano Nazionale Scuola Digitale e delle normative vigenti in materia di sicurezza online e tutela dei minori.

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.

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.

1.5 - I Piani di Azione dell'ePolicy

Finalità

Il presente Piano d'Azione ha lo scopo di:

- Promuovere un uso consapevole, sicuro e responsabile delle tecnologie digitali da parte di studenti, docenti e attori esterni;
- Prevenire e contrastare fenomeni di **bullismo e cyberbullismo**;
- Garantire la **tutela dei dati personali**, della privacy e dell'integrità psicofisica degli studenti;
- Favorire la diffusione della cultura digitale e l'inclusione attraverso percorsi formativi e pratiche educative condivise.

ATTORI COINVOLTI

Figura	Ruolo/Funzione
Dirigente Scolastico	Supervisione, coordinamento generale, attivazione procedure disciplinari e legali
Animatore Digitale	Promozione formazione interna, monitoraggio uso TIC, sensibilizzazione sui rischi digitali
Referenti Bullismo e Cyberbullismo	Coordinamento azioni preventive, raccordo con enti esterni, supporto agli studenti
Team per l'Innovazione	Supporto tecnico e metodologico alla digitalizzazione e alla diffusione delle buone pratiche
Docenti e personale scolastico	Attuazione quotidiana dell'ePolicy, segnalazione comportamenti a rischio
Studenti	Fruitori consapevoli delle tecnologie, promotori della cultura digitale sicura
Famiglie	Collaborazione educativa, corresponsabilità, supporto nella prevenzione
Enti e associazioni esterne	Conformità alle regole d'Istituto, segnalazione di criticità, attuazione di progetti in sicurezza

AREE DI INTERVENTO

Formazione e sensibilizzazione

- Percorsi formativi annuali per studenti, docenti e famiglie su:
 - Uso consapevole delle tecnologie digitali
 - Prevenzione e contrasto di bullismo e cyberbullismo
 - Educazione alla cittadinanza digitale e alla sicurezza online
- Corsi per docenti sull'uso delle TIC nella didattica e sulla gestione dei rischi digitali
- Incontri informativi per le famiglie (in presenza o online)

Norme di comportamento

- Adozione e condivisione del **Patto Educativo di Corresponsabilità**, comprensivo di sezioni dedicate al digitale
- Regolamentazione chiara dell'uso dei dispositivi personali e scolastici
- Divieto di diffusione di immagini, video, contatti privati senza consenso
- Rispetto della privacy e delle norme del GDPR
- Codici di condotta per esperti esterni e organizzazioni ospitate

Monitoraggio, controllo e intervento

- Monitoraggio periodico da parte dell'Animatore Digitale sull'uso delle TIC a scuola
- Attivazione di procedure di segnalazione (anche tramite **schede allegate**)
- Interventi tempestivi in caso di episodi critici
- Collaborazione con le Forze dell'Ordine, i Servizi Sociali e le Associazioni del territorio
- Revisione annuale dei regolamenti interni (Regolamento d'Istituto, PTOF, PdM, RAV) in ottica digitale

STRUMENTI E PROCEDURE

Strumento	Descrizione
Documento ePolicy	Linee guida ufficiali condivise e approvate dagli organi collegiali
Patto Educativo	Include impegni reciproci su uso della tecnologia e comportamenti corretti
Scheda di segnalazione	Modulo da compilare per episodi sospetti o accertati di uso improprio delle TIC
Informativa agli enti esterni	Documento sintetico contenente le regole da rispettare
Registro delle attività formative	Tracciamento delle azioni di formazione e prevenzione realizzate
Casellario giudiziale (facoltativo)	Può essere richiesto agli attori esterni per tutelare i minori

Sintesi del Piano d'Azione ePolicy d'Istituto

L'ePolicy dell'Istituto definisce le regole, le responsabilità e le azioni per promuovere un uso consapevole, sicuro e responsabile delle tecnologie digitali da parte di tutta la comunità scolastica.

Obiettivi principali

- Educere a un uso corretto delle TIC
- Prevenire e contrastare bullismo e cyberbullismo
- Tutelare la privacy e la sicurezza degli studenti, in particolare dei minori
- Stabilire comportamenti e regole chiare per tutti gli attori interni ed esterni

Attori coinvolti

- Dirigente scolastico, docenti, studenti, famiglie

- Animatore digitale, referenti bullismo/cyberbullismo
- Esperti esterni, enti e associazioni

Azioni previste

- Formazione per studenti, docenti e famiglie sull'uso sicuro del digitale
- Diffusione del Patto Educativo di Corresponsabilità e dell'ePolicy
- Obbligo per gli attori esterni di rispettare regole sull'uso dei dispositivi e la privacy
- Possibilità di richiedere il casellario giudiziale a chi lavora a contatto con minori
- Attivazione di procedure di segnalazione per comportamenti inappropriati

Strumenti operativi

- Documento ufficiale di ePolicy pubblicato sul sito della scuola
- Scheda di segnalazione per uso improprio delle tecnologie
- Codici di condotta per esperti e organizzazioni esterne
- Esposizione del documento in punti visibili dell'Istituto

Verifica e aggiornamento

Il piano viene rivisto ogni anno, in base a nuove normative, emergenze o buone pratiche emerse.

Piano d'Azione ePolicy – Versione Tabellare

Azione	Responsabile/i	Destinatari	Obiettivo	Strumenti
Condivisione ePolicy	Dirigente scolastico, Animatore Digitale	Tutta la comunità scolastica	Informare e coinvolgere	Pubblicazione sul sito, sul Registro Elettronico e sui canali istituzionali, Patto di Corresponsabilità,
Formazione sul digitale	Animatore Digitale, Referenti Cyberbullismo	Docenti, studenti, famiglie	Uso consapevole delle TIC	Incontri, workshop, moduli online
Prevenzione bullismo e cyberbullismo	Referenti di Istituto, DS	Studenti e famiglie	Tutela e sicurezza	Progetti, incontri con esperti e Forze dell'Ordine
Regolamento per enti e professionisti esterni	DS, Funzioni Strumentali	Associazioni, esperti, formatori	Garanzia di comportamenti corretti	Condivisione e sottoscrizione ePolicy, eventuale richiesta casellario
Attivazione procedure di segnalazione	Tutti gli attori coinvolti	Personale interno ed esterno	Rapida presa in carico di situazioni a rischio	Scheda di segnalazione, contatti referenti
Monitoraggio e aggiornamento	Commissione Innovazione, Team Digitale	Intero Istituto	Miglioramento continuo	Revisione annuale, raccolta buone pratiche

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

Kit Didattico

Area formazione (per docenti, famiglie, studenti/sse con ePolicy)

Canale [Youtube](#)(webinar, video-stimolo, serie per target differenti)

Canale [TikTok](#)

Canale [Instagram](#)

Canale [Facebook](#)

Cap 2 - Sensibilizzazione e prevenzione

2.1 - Sensibilizzazione e prevenzione

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 rischio online per i minori si manifesta quando:

- compiono azioni che possono danneggiare sé stessi o altri;
- ne sono vittime;
- assistono a comportamenti dannosi altrui.

Riconoscere, distinguere e comprendere questi fenomeni è fondamentale per contrastarli efficacemente. La prevenzione non si limita a intervenire dopo che un problema si è manifestato, ma agisce in anticipo, riducendo i fattori di rischio e rafforzando le competenze personali.

Due strumenti fondamentali:

1. **Sensibilizzazione:** mira a far comprendere i rischi, fornendo conoscenze e proponendo comportamenti adeguati.
2. **Prevenzione:** si traduce in attività concrete che promuovono le competenze digitali e favoriscono un uso sicuro e consapevole della rete.

Docenti, studenti e famiglie devono sviluppare:

- una consapevolezza critica dei servizi digitali;
- la capacità di riconoscere e segnalare situazioni rischiose;
- un approccio attivo alla cittadinanza digitale.

Il valore dell'ePolicy.

L'ePolicy è lo strumento guida per costruire una scuola digitale sicura. Rappresenta un patto educativo tra tutti i membri della comunità scolastica, promuovendo diritti, doveri e responsabilità online. Attraverso essa, la scuola si impegna a educare cittadini digitali consapevoli, rispettosi e protetti.

2.2 - Il Curricolo Digitale

L'Istituto Tecnico Economico e Tecnologico "Gaetano Salvemini" si distingue per un approccio pionieristico all'innovazione didattica, avendo adottato da oltre 13 anni un modello educativo centrato sull'uso individuale dell'iPad per ogni studente. Questa scelta ha trasformato l'intera esperienza scolastica, integrando profondamente la tecnologia nei processi di insegnamento e apprendimento. Si conferma quindi come un punto di riferimento nell'adozione di pratiche didattiche innovative, integrando tecnologia, competenze digitali e attenzione alla sicurezza online. Il suo curricolo digitale, supportato dall'uso del tablet nella didattica quotidiana e guidato da un solido documento di ePolicy, prepara gli studenti a essere protagonisti consapevoli e competenti nel mondo digitale contemporaneo. Questo modello ha trasformato l'ambiente scolastico in un ecosistema digitale dinamico, favorendo l'engagement, la motivazione e l'autonomia degli studenti. Infatti questo ha permessi di:

- **Personalizzazione dell'apprendimento:** adattando i contenuti alle esigenze individuali.
- **Accesso a risorse digitali:** libri di testo interattivi, app educative e piattaforme online.
- **Sviluppo di competenze trasversali:** come il pensiero critico e la creatività.
- **Collaborazione in tempo reale:** attraverso strumenti di condivisione e comunicazione.

Competenze e innovazione

Il curricolo digitale dell'ITET Salvemini è progettato per sviluppare competenze digitali avanzate, in linea con il framework europeo DigComp 2.2 finalizzato ad acquisire abilità specifiche e a sviluppare un approccio critico ed un pensiero computazionale.

- **Alfabetizzazione su informazioni e dati:** ricerca, valutazione e gestione di contenuti digitali.
- **Comunicazione e collaborazione:** interazione efficace attraverso piattaforme digitali.
- **Creazione di contenuti digitali:** produzione e condivisione di materiali multimediali.
- **Sicurezza:** utilizzo consapevole e sicuro delle tecnologie.

- **Risoluzione di problemi:** affrontare e risolvere situazioni complesse in ambienti digitali

Questo approccio mira a preparare gli studenti non solo all'uso competente della tecnologia, ma anche a una cittadinanza digitale responsabile.

Conclusione

Il curricolo digitale dell'ITET "Gaetano Salvemini" di Molfetta è parte integrante del curricolo d'Istituto; è il risultato di un lungo e strutturato percorso con radici profonde che hanno permesso una trasformazione culturale e metodologica nella didattica curriculare.

Questa esperienza si è consolidata nel tempo attraverso una progettazione consapevole e progressiva delle competenze digitali, in linea con i principali riferimenti normativi ed europei. Il DigComp 2.2, il Piano Nazionale Scuola Digitale e le Linee guida ministeriali sulla certificazione delle competenze hanno fornito le fondamenta teoriche su cui si è costruito un curricolo che non si limita all'aspetto tecnico dell'uso delle tecnologie, ma punta a formare cittadini digitali responsabili, critici e consapevoli.

L'approccio del Salvemini è infatti trasversale e interdisciplinare: ogni disciplina contribuisce a promuovere l'alfabetizzazione digitale, integrando nei propri obiettivi attività e contenuti specifici che stimolino il pensiero critico, la creatività, la sicurezza online e la capacità di risolvere problemi attraverso le tecnologie. Il digitale non è un contenuto a sé stante, ma un vero e proprio strumento trasversale di apprendimento e cittadinanza.

In questo contesto, il documento di ePolicy assume un ruolo centrale: non solo orienta le scelte educative della scuola in tema di sicurezza, privacy e benessere digitale, ma rappresenta anche la base per progettare laboratori, incontri e momenti di riflessione condivisa tra studenti, docenti, famiglie e territorio. Ogni classe, ogni anno, affronta attività calibrate per età e contesto, facendo leva su un kit didattico dedicato e valorizzando l'apporto di partner esterni come università, enti locali, associazioni e imprese.

Il curricolo digitale del Salvemini è quindi un progetto dinamico e partecipato, che evolve insieme alla scuola, aprendosi a sperimentazioni e innovazioni che rendono l'esperienza educativa più coinvolgente, inclusiva e significativa per tutti. La tecnologia, in questa visione, non è mai fine a sé stessa, ma uno strumento per costruire relazioni, conoscenza e senso di responsabilità verso il mondo che ci circonda.

2.3 - Il Kit Didattico

L'e-Policy dell'ITET Salvemini si articola su due livelli: uno istituzionale, che coinvolge tutta la comunità scolastica nella condivisione di principi e obiettivi comuni sul digitale, e uno operativo, centrato sulle singole classi, chiamate ad affrontare tematiche complesse legate alla sicurezza online come etica digitale, algoritmi e datafication. A supporto, si utilizzano i materiali di **Generazioni Connesse**, utili per strutturare attività educative efficaci. Il kit didattico è flessibile e modulare, costruito su cinque aree chiave: trasformazioni digitali, impatti sociali, educazione all'informazione, logiche dei dati e creatività digitale. Il kit può essere utilizzato nella sua interezza oppure essere oggetto di selezione e scelta, sulla base di quanto fatto dal docente.

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

3.1 - Protezione dei dati personali e GDPR

La protezione dei dati personali delle persone fisiche costituisce un diritto fondamentale. L'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea e l'art. 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Le principali normative di riferimento sono: il Regolamento Generale sulla Protezione dei Dati 2016/679 noto anche come GDPR, e il Dlgs 196/2003 conosciuto come Codice Privacy. Il settore dell'istruzione è particolarmente impattato dalla tematica privacy in considerazione del fatto che gli Istituti Scolastici sono chiamati, necessariamente, a trattare un'enorme mole di dati personali. Con l'entrata in vigore del GDPR è stato introdotto l'obbligo per ciascun Istituto scolastico di provvedere alla designazione di un Responsabile della protezione dei dati personali (RPD o DPO).

3.2 - Strumenti di comunicazione online (PUA)

La Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) è un documento che racchiude una serie di regole legate all'utilizzo della rete a scuola e a casa da parte di studenti e di tutto il personale (compresi i professionisti esterni che lavorano in contesto scolastico), integrante il DPS (Documento programmatico sulla Sicurezza). Il documento, che funge da raccordo, si compone di punti strategici riguardanti non solo i vantaggi di internet a scuola ma anche i rischi connessi all'online, nella valutazione di quei contenuti presenti in rete e di quelle azioni negative che possono comprometterne l'uso positivo. Fra queste attività: ricercare materiale non consono allo stile educativo della scuola; produrre vere e proprie azioni illecite; giocare online con la rete scolastica; violare la privacy e i diritti d'autore, etc... Nella Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) vengono definite, dunque, le regole di utilizzo fra tutti gli attori in gioco, nel rispetto dei dati sensibili di ciascuno, in particolar modo degli alunni. Bisogna comunque tener presente che 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 recita che: *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale. 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. Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete. L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite. 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.* 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".

L'accesso a Internet è dunque un diritto 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.

L'utilizzo dei dispositivi informatici in dotazione all'istituto viene regolamentato nel seguente modo: 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: per i dispositivi in dotazione all'istituto che hanno 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 dai referenti designati dal Dirigente Scolastico.

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 gli alunni si impegnano: • 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 e riposto nell'apposito contenitore lo smartphone durante le attività didattiche che non ne prevedano l'utilizzo specifico • 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, profili sui social network (Facebook, Instagram e Youtube). 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, Piattaforma GSuite (Classroom, Meet, Gmail).

• **Il Registro Elettronico -CLASSEVIVA di Spaggiari.** Tutti hanno a disposizione un account personale per l'accesso ai servizi. Tutte le comunicazioni relative a circolari, autorizzazioni, provvedimenti disciplinari, programmazioni ecc. vengono veicolati attraverso questo strumento e nulla viene pubblicato sul sito. Inoltre i docenti possono anche condividere con gli alunni contenuti didattici.

• **G Suite di GOOGLE** quale piattaforma per comunicare, svolgere incontri sincroni, condividere contenuti digitali. Gli studenti, i docenti ed i genitori devono tuttavia sapere, nel momento in cui ricevono le credenziali di accesso e dopo aver accettato la 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 e Telegram, 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, 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; • Evitare il più possibile di condividere foto di studenti in chat; • Evitare messaggi

troppo spezzettati, cercando il più possibile di essere brevi ed esaustivi allo stesso tempo;

Cap 4 - Segnalazione e gestione dei casi

Le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti rappresentano 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.

4.1 - Cosa Segnalare

Vengono qui indicate le problematiche a cui fanno riferimento le procedure indicate:

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/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 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.

4.2 - 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, che rimuoverà i contenuti entro 48 ore.

Sono a disposizione i seguenti servizi:

- Servizio di Helpline 19696
- Chat di Telefono Azzurro per supporto ed emergenze www.azzurro.it;

Si deve considerare che l'insegnante riveste la qualifica di pubblico ufficiale (ex art. 357 c.p.) in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative. Il Codice Penale Italiano, all'art. 357, definisce il pubblico ufficiale come colui che esercita una "pubblica funzione legislativa, giudiziaria o amministrativa". Questa definizione si estende ai docenti nel momento in cui sono impegnati nell'esercizio delle loro funzioni all'interno degli istituti scolastici. La Corte di Cassazione, con la sentenza n. 15367/2014, ha ribadito la qualifica di pubblico ufficiale per l'insegnante, estendendo tale riconoscimento non solo alla tenuta delle lezioni, ma anche a tutte le attività connesse. Questo include, ad esempio, gli incontri con i genitori degli allievi. Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite da un team di docenti composto da:

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

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

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

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

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l'obiettivo di allertare il Dirigente. La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, si procede alla valutazione approfondita e alla verifica di quanto segnalato, avviando (se appurato la rilevanza penale) la procedura giudiziaria con denuncia all'autorità giudiziaria per attivare un procedimento penale. Qualora si rilevasse un fatto riconducibile alla fattispecie di reato, l'insegnante - nel ruolo di pubblico ufficiale – non deve procedere con indagini di accertamento ma ha sempre l'obbligo di segnalare l'evento all'autorità giudiziaria. (ex. l. 71/2017). Con autorità competente si intendono:

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

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

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

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

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

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

Gli insegnanti e i genitori, come studenti e studentesse, si possono rivolgere alla Helpline del progetto Generazioni Connesse, al numero gratuito 19696, attraverso la chat disponibile sul [sito](#) o tramite chat WhatsApp per ricevere supporto e consulenza.

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, può essere necessario rivolgersi ad altre figure, enti, istituzioni e servizi presenti sul territorio qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola. Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso. 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. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- 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 e studentesse

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

Allegati con le procedure

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo



Il docente ha evidenza che sta 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 quattordicenne 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.

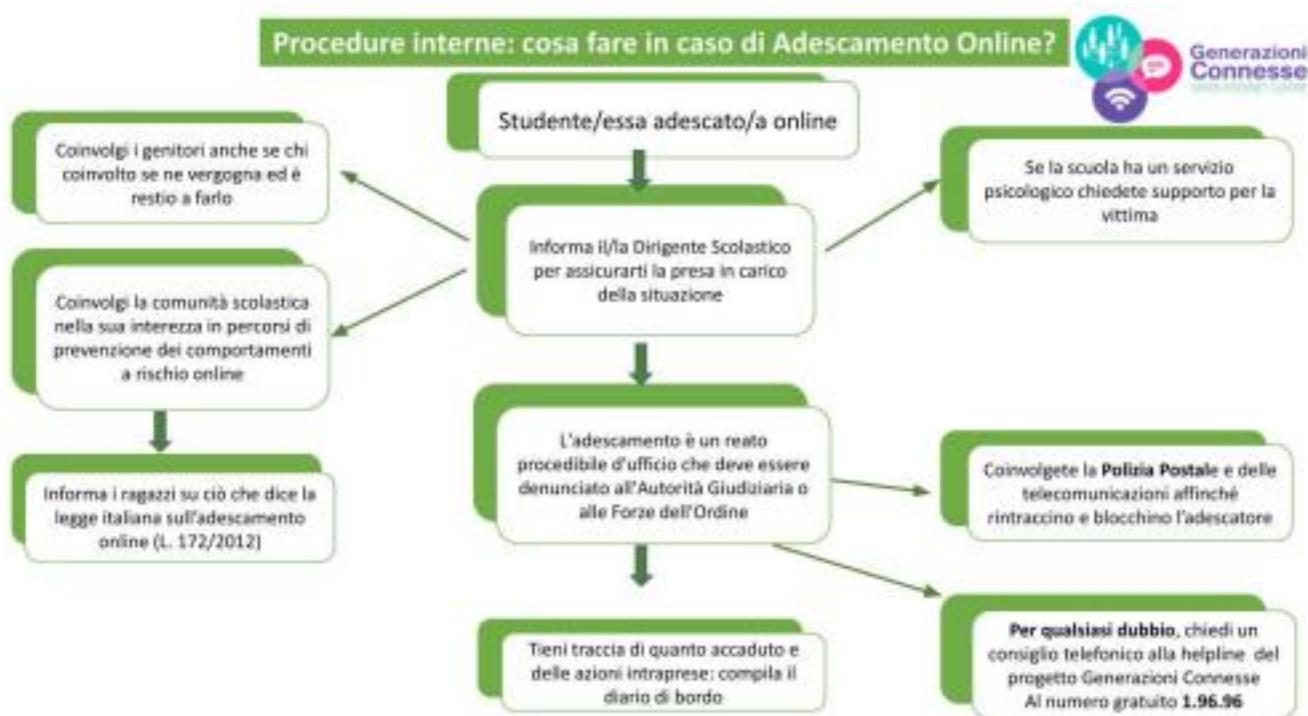
NELLE CLASSI

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 adescamento online?



Procedure interne: cosa fare in caso di sexting?

