



Istituto di Istruzione Superiore
"VANVITELLI STRACCA ANGELINI"

Via Umberto Trevi, 4 - 60127 Ancona - Tel. 071 4190711 - Fax 071 4190712
C.F. 93084450423 - Cod. meccanografico ANIS00400L - Sito <https://istvas.edu.it>
email: anis00400l@istruzione.it - anis00400l@pec.istruzione.it - scuola@istvas.edu.it
Codice univoco fatturazione UF01E9 - Codice IPA: istsc_anis00400L



INDIRIZZI DI STUDIO: Agraria Agroalimentare e Agroindustria - Chimica, Materiali e Biotecnologie (Ambientali e Sanitarie) - Costruzioni, Ambiente e Territorio - Sistema Moda

Circolare n. 0353

Ancona, 19.01.2026

A tutti i docenti
Agli alunni e alle famiglie
Alla DSGA
Al personale ATA

Oggetto: redazione documento e-policy e riconoscimento attestato "Scuola Virtuosa"

Si comunica a tutte le componenti della comunità scolastica che il nostro Istituto ha conseguito l'attestato di «**Scuola Virtuosa**» ed è stato iscritto nell'albo ufficiale della piattaforma **SIC – Generazioni Connesse**.

Tale riconoscimento è stato ottenuto grazie al lavoro svolto dai docenti del **Team della Digitalizzazione e dell'Intelligenza Artificiale** – proff. Augello, Nocera, Pavani, Renghini e Toccaceli – coordinati dalla prof.ssa De Cata, che hanno portato a termine il corso di formazione previsto dal progetto, culminato nella redazione del documento di **e-Policy** dell'Istituto.

Il documento di e-Policy non ha carattere statico, bensì dinamico, in quanto potrà essere aggiornato annualmente; esso rappresenta, tuttavia, un impegno formale dell'Istituto nella formazione, educazione e informazione di tutti gli utenti in merito a un utilizzo sicuro e consapevole della rete. Il documento sarà pubblicato sul sito web istituzionale.

Si ricorda inoltre che l'Istituto è iscritto alla piattaforma **SIC – Generazioni Connesse** (<https://www.generazioniconnesse.it/site/>), all'interno della quale sono disponibili:

- ✓ percorsi di formazione rivolti a docenti, genitori e studenti;
- ✓ progetti di cittadinanza digitale utilizzabili come percorsi e contenuti per l'insegnamento dell'Educazione civica.

In allegato alla presente si trasmettono il documento di e-Policy redatto e l'attestato di «**Scuola Virtuosa**» conseguito.

IL DIRIGENTE SCOLASTICO

Prof. Ing. Francesco Savore

(Firma autografa sostituita a mezzo stampa
ai sensi dell'art.3, comma 2 del D.Lgs. n.39/1993)





Documento di ePolicy VANVITELLI - STRACCA - ANGELINI

VIA U. TREVI 4 - 60131 - ANCONA
Ancona (AN) - Marche
Data di approvazione: 15/01/2026 - 22:37

Cap 1 - Lo scopo della ePolicy

1.1 Scopo della ePolicy

Capitolo 1 - Presentazione dell'ePolicy

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

Capitolo 2 - Sensibilizzazione e prevenzione

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

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

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

Capitolo 4 - Segnalazione e gestione dei casi

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

1.1 Scopo dell'ePolicy

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

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

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

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

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

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

L'Istituto Vanvitelli Stracca Angelini, consapevole dei problemi che possono derivare da un uso scorretto ed incauto della rete si attiva per attuare attività di prevenzione, controllo e formazione di studentesse, studenti e famiglie allo scopo di ridurre al minimo l'occorrenza di atti che non solo creano disagio nella comunità scolastica, ma possono configurarsi come veri e propri reati.

La scuola opera in stretto collegamento con le forze dell'ordine, come la Polizia Postale Telematica, con la Procura della Repubblica, con istituzioni del settore educativo ed Enti Locali, per mettere in campo strategie di prevenzione di episodi di cyberbullismo e interventi di recupero nel caso in cui vengano individuati tali fenomeni, informando i genitori/tutori e chiedendo la loro collaborazione anche qualora gli episodi si siano verificati al di fuori delle attività didattiche.

Per evitare che l'adozione di questa policy rappresenti un mero atto formale, l'Istituto si impegna a prendere spunto da essa come base di partenza per una serie di azioni e iniziative. A partire dalla pubblicazione sul sito della scuola del presente documento, si prevedono le seguenti azioni:

- discussione collegiale sui contenuti, sulle pratiche indicate, per il corpo docente e il personale ATA (nelle sedi competenti);
- eventuale revisione, su base annuale, circa la necessità di apportare modifiche e miglioramenti alla policy vigente a seguito di segnalazioni ricevute dalle varie componenti;
- discussione in classe della policy nei primi giorni di scuola, con particolare riguardo al protocollo di accoglienza per le nuove classi prime, per la componente studentesca;
- inserimento di un estratto di questo documento nel vademecum degli studenti e delle studentesse;
- organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare per i genitori.

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

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

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

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

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

IL DIRIGENTE SCOLASTICO

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

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

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

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

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

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

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

In coerenza con le Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo del Ministero dell'Istruzione (D.M. n. 18 del 13/1/2021, agg. 2021 – nota prot. 482 del 18-02-2021), il Team ha le funzioni di coadiuvare il Dirigente Scolastico, coordinatore del Team nella scuola, nella definizione degli interventi di prevenzione e nella gestione dei

casi di bullismo e cyberbullismo che si possono presentare. Promuove inoltre la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale e comunica ad alunni, famiglie e tutto il personale scolastico dell'esistenza del team, a cui poter fare riferimento per segnalazioni o richieste di informazioni sul tema.

Il Team ha il compito di:

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

I/LE DOCENTI

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

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

RESPONSABILE DELLA PROTEZIONE DEI DATI

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

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

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

GLI STUDENTI E LE STUDENTESSE

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

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

I GENITORI/ADULTI DI RIFERIMENTO

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

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

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

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

In particolare per l'IIS Vanvitelli Stracca Angelini si sottolinea che:

IL DIRIGENTE SCOLASTICO

È responsabile della presentazione di questo documento all'attenzione del Collegio dei Docenti e all'approvazione del Consiglio di Istituto; deve anche valutare l'efficacia delle azioni intraprese e monitorarne l'attuazione, anche in collaborazione con personale scolastico, enti locali e referenti territoriali.

A tale scopo necessita di ricevere tempestive informazioni sulle violazioni al presente regolamento o eventuali problemi attualmente non noti dal corpo docente o dal personale ATA che ne vengano a conoscenza.

L'ANIMATORE DIGITALE E IL TEAM DELLA DIGITALIZZAZIONE E DELL'IA

Cura la redazione iniziale e l'eventuale revisione annuale della policy sulla base delle osservazioni ricevute da tutti i soggetti interessati; ne assicura la massima diffusione dentro la comunità scolastica in tutte le sue componenti (docenti/personale ATA, genitori e studenti), mediante pubblicazione sul sito della scuola. Si relaziona con l'Ufficio Tecnico e l'Amministratore di

rete per definire le misure di sicurezza informatica più opportune; riferisce al Dirigente Scolastico situazioni o problemi di particolare rilevanza su cui intervenire.

I REFERENTI PER IL BULLISMO E IL CYBERBULLISMO

Hanno il compito di coordinare le iniziative di prevenzione e contrasto del bullismo e del cyberbullismo. A tal fine, i referenti di istituto possono avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio. E condividere con tutta la comunità scolastica la legge **"linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo"** e il Regolamento di Istituto per la prevenzione e il contrasto dei fenomeni di Cyberbullismo e bullismo approvato dagli organi Collegiali e presente sul sito web dell'Istituto al seguente link:

<https://istvas.edu.it/documento/linee-di-orientamento-per-azioni-di-prevenzione-e-di-contrasto-al-bullismo-ed-al-cyberbullismo/>

IL PERSONALE DOCENTE E IN PARTICOLARE I COORDINATORI DEI CONSIGLI DI CLASSE

Gli insegnanti sono tenuti a:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- aver letto, compreso e sottoscritto la presente policy;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'Animatore Digitale per le opportune indagini / azioni / sanzioni;
- mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici;
- integrare i problemi di sicurezza informatica in tutti gli aspetti del curriculum di studi e in altre attività extracurricolari;
- far comprendere alla componente studentesca e far mettere in pratica le regole di comportamento relative alla sicurezza informatica;
- far nascere nella componente studentesca una buona cognizione della proprietà del software e delle normative sul diritto d'autore nonché di far comprendere la necessità di effettuare ricerche sul web e la relativa estrazione di documenti evitando il plagio o l'illecita diffusione di dati personali;
- controllare l'uso delle tecnologie digitali, smartphone, dispositivi mobili, ecc. nelle lezioni e nelle altre attività scolastiche che ne prevedono la necessità a scopi didattici;
- guidare la navigazione di alunni/alunne nelle lezioni in cui l'uso di Internet è pianificato, verso siti controllati come idonei per il loro uso, onde evitare di incontrare materiali inadatti.

IL PERSONALE ATA

Il personale ATA è tenuto a:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- aver letto, compreso e sottoscritto la presente policy;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'animatore digitale per le opportune indagini / azioni / sanzioni;
- mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici;
- controllare la presenza dell'accettazione della liberatoria ai fini della pubblicazione di foto, video degli alunni (personale della segreteria didattica) e comunicare all'Amministratore di rete l'eventuale non accettazione.

GLI STUDENTI E LE STUDENTESSE

Le alunne/gli alunni sono responsabili per l'utilizzo corretto dei sistemi informatici e della tecnologia digitale in accordo con i

termini previsti da questa policy.

In particolare sono tenuti a:

- non utilizzare dispositivi personali (smartphone, dispositivi mobili, ecc.) durante le attività didattiche se non espressamente autorizzato dal Dirigente Scolastico;
- avere una buona comprensione delle possibilità di ricerca sul web e della necessità di evitare il plagio, rispettare le normative sul diritto d'autore, non diffondere dati personali e conoscere gli elementi essenziali della Netiquette (insieme di regole, comunemente accettate e seguite da quanti utilizzano Internet e i servizi di rete, che disciplinano il comportamento di un utente nel rapportarsi agli altri utenti attraverso risorse come mailing list, forum, blog o e-mail);
- comprendere l'importanza della segnalazione di ogni abuso, uso improprio o accesso a materiali inappropriati informando tempestivamente il coordinatore di classe;
- capire le politiche di utilizzo delle immagini ed essere consapevoli del significato e della gravità del cyberbullismo;
- capire l'importanza di adottare buone pratiche di sicurezza informatica in tutti i momenti della vita, a tutela dell'incolumità propria e altrui e per evitare di perpetrare reati punibili sia a livello scolastico sia da parte della magistratura.

I GENITORI E I TUTORI

Genitori e tutori svolgono un ruolo cruciale nel garantire che i propri figli comprendano l'importanza di un utilizzo corretto, sicuro e responsabile della rete Internet e delle tecnologie digitali.

La scuola, consapevole della rilevanza educativa di tali tematiche, si impegna a cogliere ogni occasione utile per sensibilizzare e informare le famiglie sui rischi e sulle opportunità del mondo digitale, attraverso:

- incontri informativi e formativi con la Polizia Postale e con altri esperti, educatori o professionisti del settore;
- pubblicazione di circolari e comunicazioni ufficiali;
- materiali informativi e approfondimenti pubblicati sul sito istituzionale della scuola, in apposite sezioni dedicate.

I genitori saranno incoraggiati a collaborare attivamente con la scuola nella promozione delle buone pratiche di eSafety, nonché a rispettare e far rispettare ai propri figli le linee guida relative all'uso appropriato di:

- immagini digitali e video realizzati in occasione di eventi scolastici, anche al di fuori delle aule, nel rispetto della privacy e della normativa vigente;
- sezioni del sito web della scuola riservate alle famiglie, con particolare riferimento al registro elettronico;
- dispositivi digitali personali degli studenti all'interno dell'ambiente scolastico.

A tale scopo per favorire la crescita civile, sociale e digitale degli studenti tra le famiglie e la scuola viene sottoscritto il Patto di corresponsabilità Educativa disponibile al seguente link:
<https://istvas.edu.it/documento/patto-educativo-corresponsabilita/>

In tale patto in particolare:

- La scuola si impegna a promuovere un uso consapevole e sicuro delle tecnologie digitali, a prevenire comportamenti scorretti o rischiosi in rete e a intervenire con azioni educative adeguate in caso di necessità.
- Le famiglie si impegnano a vigilare sull'utilizzo delle tecnologie da parte dei propri figli, a dialogare con loro sui rischi e sulle responsabilità connesse all'uso di Internet e a collaborare con la scuola nel rispetto delle regole condivise.

SOGGETTI ESTERNI - ENTI -ASSOCIAZIONI

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori

che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

1.3 Integrazione ePolicy nei documenti scolastici

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

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

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

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

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

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

Per l'IIS Vanvitelli Stracca Angelini il presente documento una volta approvato negli Organi Collegiali proposti: Collegio Docenti e Consiglio di Istituto andrà a integrare i seguenti documenti:

- Regolamento di Istituto
- Patto di Corresponsabilità
- PTOF triennale

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

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

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

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

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

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

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

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

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

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

1.5 - I Piani di Azione dell'ePolicy

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

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

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

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

1° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

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

MODULO II

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

MODULO III

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

MODULO IV

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

2° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

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

MODULO II

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

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

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

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

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

L'Istituto "Vanvitelli Stracca Angelini" per gli studenti e le studentesse promuove l'accesso agli strumenti digitali e si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educarli verso un uso consapevole e responsabile delle tecnologie digitali come parte integrante della loro esperienza di apprendimento e quindi far maturare in loro le competenze per una proficua cittadinanza digitale. Ciascun Consiglio di Classe avrà cura di strutturare il proprio piano di lavoro in modo da agevolare negli studenti l'acquisizione di competenze digitali. A tale scopo l'Istituto si è dotato di Curricolo Digitale reperibile al seguente link: <https://istvas.edu.it/documento/curricolo-digitale-verticale/>

Per la formazione del corpo docente, essa sarà organizzata su due livelli: interno ed esterno. A livello interno nel PTOF si prevede che una parte della formazione sia dedicata proprio all'uso e all'inserimento delle TIC nella didattica e ai temi informatici in generale. Tale formazione sarà coordinata dai docenti dell'Istituto che fanno parte del Team della Digitalizzazione e dell'IA e sarà improntata anche nella condivisione di esperienze significative e di buone pratiche. Per quanto riguarda la formazione esterna, la scuola assicura tempestiva e capillare informazioni su: corsi, seminari e convegni che riguardino tali argomenti, cercando altresì di agevolare il personale docente che intende partecipare. Inoltre l'Istituto, per quanto possibile favorirà l'adesione di docenti e alunni appositi presentati da enti e associazioni certificate.

2.2 - Il Curricolo Digitale

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

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

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

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

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

L'Istituto "Vanvitelli Stracca Angelini" ha approvato nel precedente a.s. il Curriculum Digitale presente al seguente link:
<https://istvas.edu.it/documento/curricolo-digitale-verticale/>

Lo scopo del documento, rivolto in particolare agli alunni del primo biennio, è quello di sollecitare all'interno di ciascun consiglio di classe lo sviluppo di percorsi volti a promuovere competenze di cittadinanza digitale attraverso l'accesso agli strumenti digitali che educano gli studenti e le studentesse anche ad un uso consapevole e responsabile delle tecnologie digitali

Per la formazione del corpo docente, così come programmato nel PTOF, verranno attivati percorsi su due livelli: interno ed esterno. A livello interno la formazione sarà improntata da una parte sulla condivisione delle esperienze e delle buone pratiche in modalità peer-learning con il supporto del Team della "Digitalizzazione e dell'IA" e dall'altra parte verranno attivati corsi di formazione svolti da personale esperto esterno opportunamente selezionato

Per quanto riguarda la formazione esterna la scuola assicura ed assicurerà tempestiva informazione su corsi e convegni riguardanti l'approfondimento delle tecnologie digitali nella didattica e cercherà di agevolare la partecipazione del proprio personale scolastico a percorsi di formazione presentati da enti ed associazioni esterne certificate.

2.3 - Il Kit Didattico

L'e-Policy prevede, a livello macro, un lavoro di lettura e d'intenti condivisi dall'intera comunità scolastica, a livello micro, invece, immagina che la singola classe lavori anche su tematiche direttamente collegate alla sicurezza in rete, ma complesse e di non immediata ricaduta nelle programmazioni scolastiche (etica e digitale, algoritmi, datafication). A tal fine si è progettato e predisposto del materiale che possa funzionare sia da attivatore, sia d'accompagnamento ai docenti e agli studenti nella fase più delicata ed incisiva del processo di prevenzione: la lezione in classe.

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

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

3.1 - Protezione dei dati personali e GDPR

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

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

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

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

Il nostro Istituto è dotato di una rete fisica cablata e di una rete wireless con protocollo wi-fi.

Navigazione in internet: filtri e antivirus

Il nostro Istituto, sia per la rete wi-fi che per la rete cablata, utilizza antivirus di sistema e antivirus di terze parti, costantemente aggiornati ma è demandato ad ogni singolo utilizzatore di provvedere alla protezione del proprio dispositivo. Occorre, inoltre, sensibilizzare tutta la comunità scolastica sull'opportunità di mantenere aggiornati sia gli antivirus installati che il sistema operativo sulle macchine personali (notebook, netbook, tablet e smartphone) e controllare i dispositivi di archiviazione esterna che vengano collegati ai propri dispositivi.

Gestione accessi.

L'Istituto attualmente è dotato di una rete wireless destinata all'utilizzo didattico da parte del corpo docente, L'abilitazione all'accesso della rete avviene previo invio del MAC address (detto anche indirizzo fisico) dei dispositivi personali e consegna di una password unica a livello di Istituto allo scopo di estendere il servizio e permettere al personale in oggetto di accedere a contenuti e materiali in rete e permettere l'applicazione di una didattica innovativa e più coinvolgente per gli studenti ad essi affidati. Al contrario per gli alunni l'accesso alla rete internet, utilizzando la rete cablata, è permesso nei laboratori, nelle aule digitali e negli spazi adibiti attraverso l'abilitazione all'accesso tramite l'account personale. Tale modalità ha lo scopo di monitorare meglio eventuali usi impropri e utilizzare in maniera efficace e consapevole i contenuti della rete per utenti che ancora non hanno acquisito la maturità psicologica per valutare gli effetti negativi che azioni non consone possono provocare.

Ciascun utente connesso alla rete dovrà rispettare il presente regolamento e la legislazione vigente, tutelare la propria privacy, quella degli altri utenti adulti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui ha accesso e rispettare la cosiddetta Netiquette.

La componente studentesca e tutto il personale, dovrà impegnarsi a rispettare le norme di buon utilizzo che la scuola si impegna a redigere e a divulgare prima che sia concesso l'accesso a Internet.

E-mail.

L'Istituto fornisce una casella di posta elettronica "utente@istvas.edu.it" a tutto il personale docente, personale ATA e alla componente studentesca. Sulla rete scolastica tutti sono invitati a utilizzare solo account di posta elettronica presenti nel dominio scolastico e per scopi inerenti lo svolgimento didattico/organizzativo. Le comunicazioni tra personale scolastico, famiglie e allieve/allievi via e-mail devono avvenire preferibilmente tramite un indirizzo e-mail della scuola, per consentire l'attivazione di protocolli di controllo. E-mail in arrivo da mittenti sconosciuti vanno trattate come sospette ed eventuali allegati non devono essere aperti.

Sito web della scuola.

Il sito prevede un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali, avvisi di carattere generale, organigramma della scuola, organigramma della sicurezza, albo online ed amministrazione trasparente. Il sito web non permette interazione con l'utenza.

La scuola fa uso anche di un sito specifico per la pubblicazione del piano dell'offerta formativa finalizzato alle attività di orientamento scolastico delle classi di scuola secondaria di 1° grado.

Anche questo sito non permette l'interazione con l'utenza.

Social network.

La scuola nella pratica didattica cerca di educare la componente studentesca all'uso sicuro dei social network. Per esempio a ogni utente è consigliato di non fornire mai dati personali di alcun tipo che possano identificare con precisione le persone e la loro residenza o ubicazione. La componente studentesca non deve pubblicare senza permesso foto personali proprie o altrui su qualsiasi spazio di social network previsto nella piattaforma di apprendimento scolastico.

Registro elettronico.

Ogni famiglia riceve le credenziali per l'accesso riservato al registro elettronico, in cui il corpo docente registra assenze, valutazioni, note e osservazioni.

L'uso del registro elettronico è spiegato nel manuale pubblicato sul sito della scuola. Coloro che non possono accedere ad Internet e di conseguenza non possono consultare il registro elettronico sono pregati di darne segnalazione al coordinatore del consiglio di classe o direttamente al personale della segreteria.

Piattaforma "G-Works" per la didattica digitale integrata.

La G Workspace for Education è un insieme di applicazioni web dedicate alla comunicazione e alla collaborazione in ambiente scolastico e universitario di cui, grazie ad un accordo con Google, è possibile usufruire gratuitamente.

La G Workspace for Education ha diverse applicazioni, tra cui le più utilizzate sono:

- Gmail
- Classroom
- Meet
- Chat
- Calendar
- Drive
- Google Documenti
- Google Fogli
- Google Presentazioni

- Google Moduli

L'utilizzo della piattaforma di Google offre i seguenti vantaggi:

- sicurezza e rispetto della Privacy
- semplicità ed immediatezza operativa grazie all'ambiente di lavoro familiare (interfaccia grafica Google)
- risparmio economico (la piattaforma è gratuita)
- fruibilità e accessibilità da qualsiasi dispositivo on line (pc, tablet, smartphone), in qualsiasi parte del mondo
- possibilità di promuovere le competenze digitali degli alunni e dei docenti, di creare e usufruire di risorse, materiali e percorsi condivisi e collaborativi e di gestire uno spazio cloud di archiviazione e documentazione dei percorsi didattici e professionali.

Ad ogni studente/studentessa viene assegnato un account personale (cognome.nome@istvas.edu.it).

L'account permette l'utilizzo delle app della piattaforma di Google sopraindicate, in particolare: - la app Drive offre la possibilità di accedere alle condivisioni online di file e documentazione didattica.

- la app Calendar permette di gestire gli impegni personali e condivisi con i docenti
- la app Gmail è utilizzabile per comunicare all'interno dell'Istituto, con altri alunni e con i docenti, a scopo didattico, ed è anche disponibile per comunicazioni esterne alla scuola. - la app Meet è utilizzata per le lezioni in DID e per le riunioni video. Questa app può essere utilizzata solo all'interno del dominio@istvas.edu.it, realizzando così una modalità d'uso sicura e rispettosa della privacy.

Alle famiglie degli studenti minorenni è richiesto inoltre un impegno fattivo di collaborazione con i docenti nel responsabilizzare i ragazzi sulle modalità di accesso a internet e sulle regole a cui attenersi.

La piattaforma di Google Workspace presenta diversi livelli di sicurezza dati e tutela della Privacy. In particolare, Google integra la sua Normativa in materia con una serie di norme aggiuntive volte a garantire una maggiore protezione all'interno dell'ambiente education, quali:

- **Limitazioni sulla pubblicità.**

All'interno dei Servizi principali della piattaforma di Google, i prodotti e i servizi Google NON possono contenere annunci pubblicitari. Per gli utenti di G Workspace for Education delle scuole primarie e secondarie, Google non utilizza alcuna informazione personale (o associata a un account Google) per definire il target degli annunci.

- **Creazione di account da parte dell'amministratore.**

L'account G Workspace for Education di uno studente è un account Google creato dall'amministratore del dominio dell'istituto scolastico. Durante la creazione dell'account, l'amministratore può fornire alcuni dati personali dell'utente quali, ad esempio, nome, cognome. Google associa tali dati all'account.

- **Proprietà intellettuale.**

Google non acquisisce la proprietà dei dati degli studenti e dei docenti. Tali dati rimangono di proprietà della scuola. Pertanto, nel momento in cui l'istituzione scolastica decide di interrompere l'utilizzo della piattaforma di Google, i dati vengono restituiti alla scuola stessa.

- **Cessione dati.**

I dati sono di proprietà delle scuole che utilizzano la piattaforma di Google ed è responsabilità di Google proteggerli. Google non cede/ vende a terze parti i dati degli studenti/ docenti, e non condivide con terze parti le informazioni personali presenti nei sistemi, tranne che in rari e circostanziate eccezioni, ad esempio quando è l'utente (solo se maggiorenne) a chiedere di condividerli o se costituisce obbligo di legge.

Infine è opportuno ricordare che la piattaforma di Google è un ambiente di archiviazione e condivisione risorse e rispetta quando indicato e suggerito dal Garante della Privacy in ambito scolastico, come illustrato nel documento "La scuola a prova di privacy".

Ulteriori informazioni sono disponibili a questo indirizzo: <https://edu.google.com/why-google/privacy-security/>

LINK UTILI

Google mette a disposizione guide e supporto per gli utenti tramite l'help in linea, consultabile all'indirizzo: <https://support.google.com/>

3.2 - Strumenti di comunicazione online (PUA)

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

3.3 - BYOD

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

L'IIS Vanvitelli Stracca Angelini, tenendo conto della circolare del MIM del 16 giugno 2025 e dell'allegato 1 presente nella circolare n° 17 del 8 settembre 2025 presente sul sito

https://istvas.edu.it/wp-content/uploads/manual/pages/regolamenti/all_1_Regolamento_cellulari_tabella_sanzioni_circolareMI_M_25.pdf

non permette per gli studenti e le studentesse l'utilizzo di strumenti digitali personali (smartphone, tablet e strumenti per l'acquisizione di immagini, video e audio) se non espressamente autorizzati dal Dirigente Scolastico.

Per il personale scolastico si preferirà, quando ciò è possibile, l'impiego della strumentazione fornita dalla scuola rispetto a quella personale (portatili, pc fissi, ...); le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali. Telefoni cellulari, tablet, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate. L'uso improprio della rete è contestato al titolare delle credenziali con cui è avvenuta la comunicazione. Qualora si utilizzino a scuola dispositivi di

archiviazione esterna di proprietà personale (chiavette usb, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.

Utilizzo del laboratorio di informatica e delle postazioni di lavoro

Durante l'attività didattica è opportuno che ogni docente dia chiare indicazioni sul comportamento corretto da utilizzare in laboratorio nello specifico sull'utilizzo della rete(internet, piattaforme studenti, social ecc...), condividendo con gli studenti il "GALATEO DELLA RETE ISTVAS presente sul sito dell'Istituto al seguente link:

<https://istvas.edu.it/documento/galateo-rete-istvas-insieme-di-regole-che-disciplinano-il-comportamento-di-un-utente-della-nostra-rete-informatica/>

e facendo conoscere le regole indicate sul "Regolamento sull'uso del laboratorio" presente in ciascun laboratorio e pubblicato sul sito web dell'Istituto al seguente link:

https://istvas.edu.it/wp-content/uploads/manual/pages/regolamenti/regolamento_laboratori_vigente_21.pdf

Cap 4 - Segnalazione e gestione dei casi

4.1 - Cosa Segnalare

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

Le misure di prevenzione comprendono l'integrazione nel curriculum dei temi legati al corretto utilizzo delle TIC e di Internet: la progettazione di unità didattiche specifiche deve essere pianificata a livello di dipartimenti disciplinari, garantendo un intervento su ogni classe, anche con docenti non titolari della classe. Si demanda agli indirizzi disciplinari la scelta dei settori su cui focalizzare la formazione: a titolo di esempio il dipartimento letterario si può soffermare in particolare sugli aspetti legati all'affettività, alla socializzazione e alla cittadinanza e alla tutela del diritto di autore, quello tecnologico-scientifico-matematico sulle questioni tecniche e legate alla salute. La scuola si avvale della collaborazione di enti e associazioni per realizzare incontri rivolti alla componente studentesca e alle famiglie con l'intento di fornire ogni elemento utile alla prevenzione e alla gestione dei problemi relativi alla sicurezza informatica; le famiglie sono invitate a proporre tematiche di particolare interesse su cui la scuola focalizzerà il proprio intervento. Il nostro Istituto attiva inoltre uno sportello di ascolto al quale la componente studentesca si può rivolgere per avere consigli e sostegno psicologico anche relativamente alle tematiche del cyberbullismo. La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti.

A partire dalla corretta formazione e sensibilizzazione di tutti gli adulti coinvolti, docenti e personale ATA sono invitati a essere confidenti e custodi, diretti o indiretti, di ciò che studentesse e studenti vivono: si raccomanda di evitare ogni atteggiamento accusatorio o intimidatorio per riuscire a ricevere dai minori più fragili segnalazioni e confidenze circa situazioni problematiche vissute. I Docenti, in particolare, sono chiamati a essere anche torre di avvistamento, spazio di avamposto privilegiato delle problematiche, dei rischi, dei pericoli che gli adolescenti possono vivere e affrontare ogni giorno. Accorgersi tempestivamente di quanto accade e compiere azioni immediate di contrasto verso gli atti inopportuni - quando non illegali - diviene fondamentale per poter evitare conseguenze a lungo termine che possano pregiudicare il benessere e una crescita armonica dei soggetti coinvolti. L'insegnante, inoltre, riveste la qualifica di pubblico ufficiale (la sua funzione non è solo circoscritta 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 attività educative) e pertanto è tenuto ad informare il Dirigente Scolastico di eventuali casi di particolare gravità.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo. La gestione dei casi rilevati va differenziata a seconda della loro gravità; fermo restando che è opportuna la condivisione a livello di Consiglio di Classe di ogni episodio rilevato, anche minimo, alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe. Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e come rimediare. Nei casi più gravi e in ogni ipotesi di reato occorrerà valutare tempestivamente con il Dirigente Scolastico come intervenire.

4.2 - Quali strumenti e a chi

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

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

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

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

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

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

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

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

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

CASO B (EVIDENZA) - Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

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

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

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

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

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

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

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

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

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

Strumenti a disposizione di studenti/esse

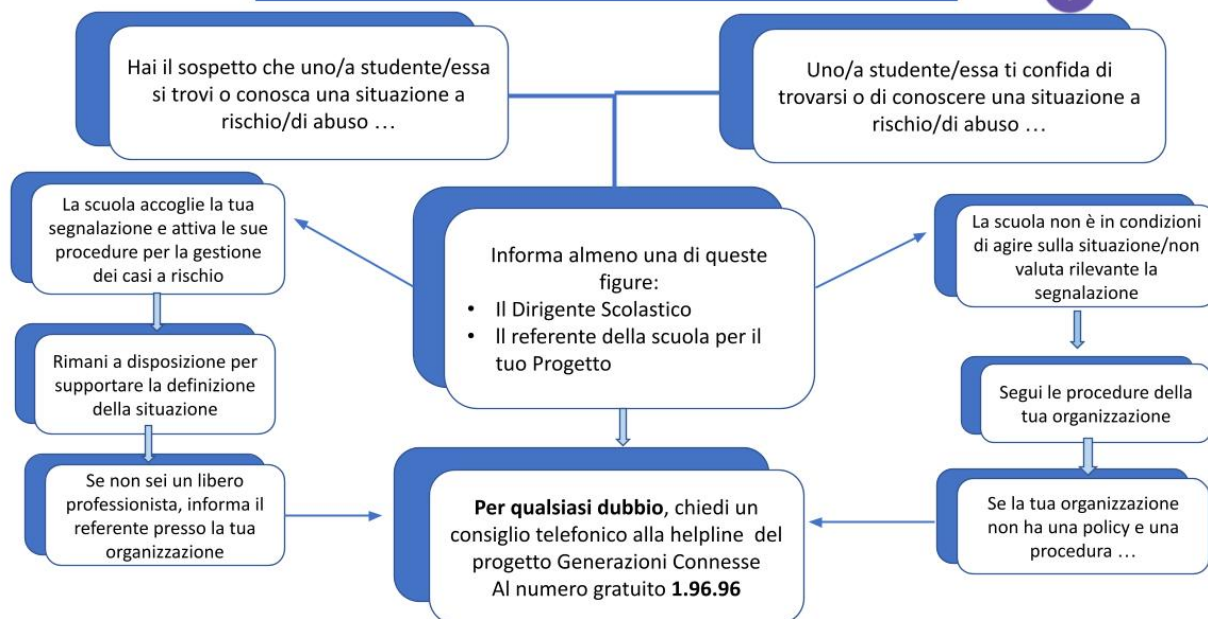
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

In particolare, sarebbe utile che la scuola attivi un sistema di segnalazione utile anche al monitoraggio dei fenomeni dal quale partire per integrare azioni didattiche preventive e giornate di sensibilizzazione, insieme agli Enti/Servizi presenti sul territorio di riferimento. Importante, altresì, immaginare e programmare percorsi di peer education per la prevenzione e il contrasto degli agiti.

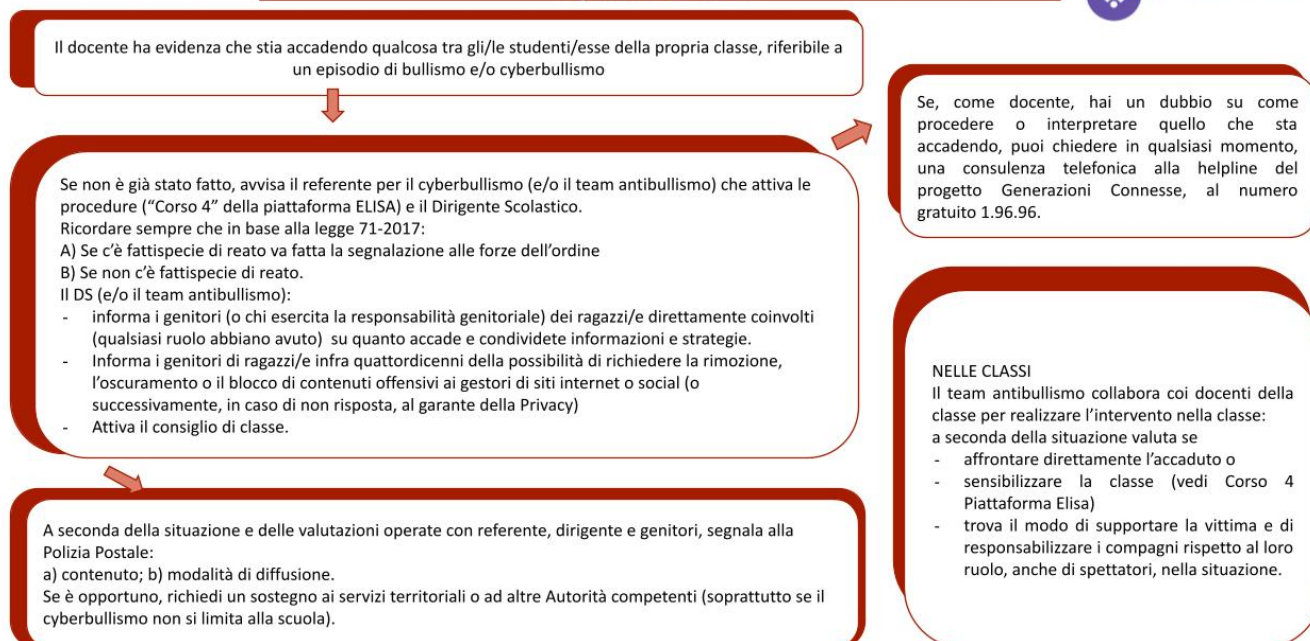
Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle [Linee di Orientamento per la prevenzione e il contrasto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

Procedure

Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola



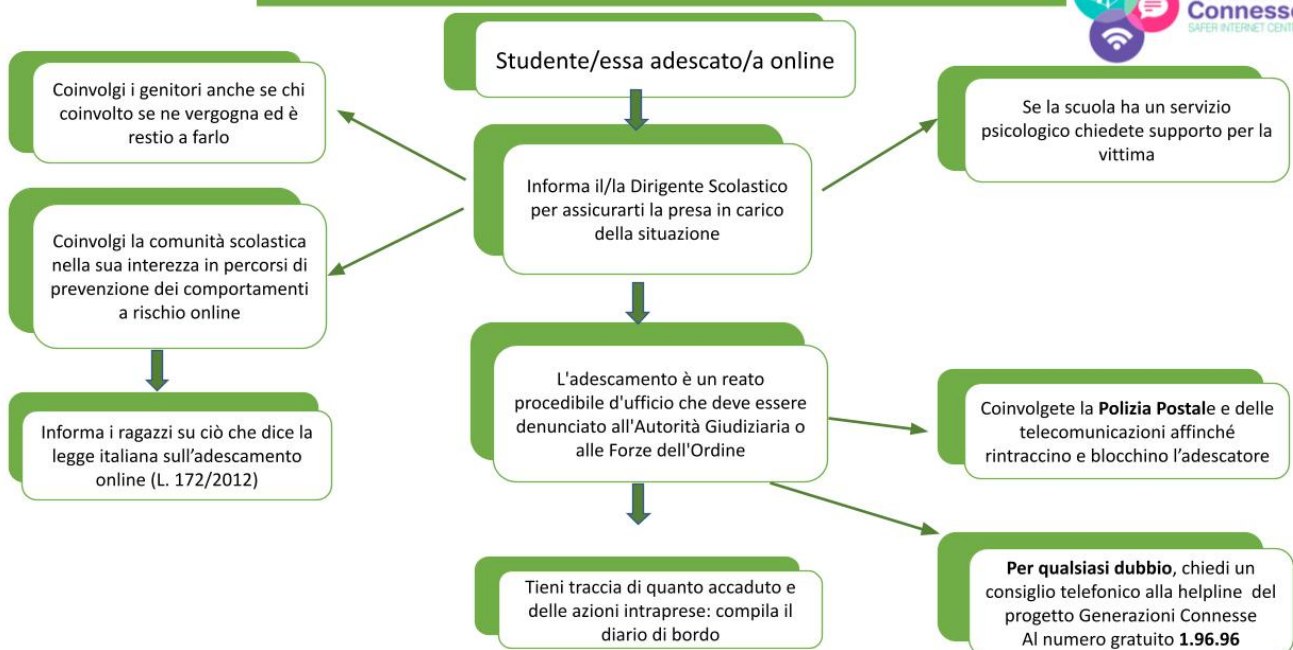
Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

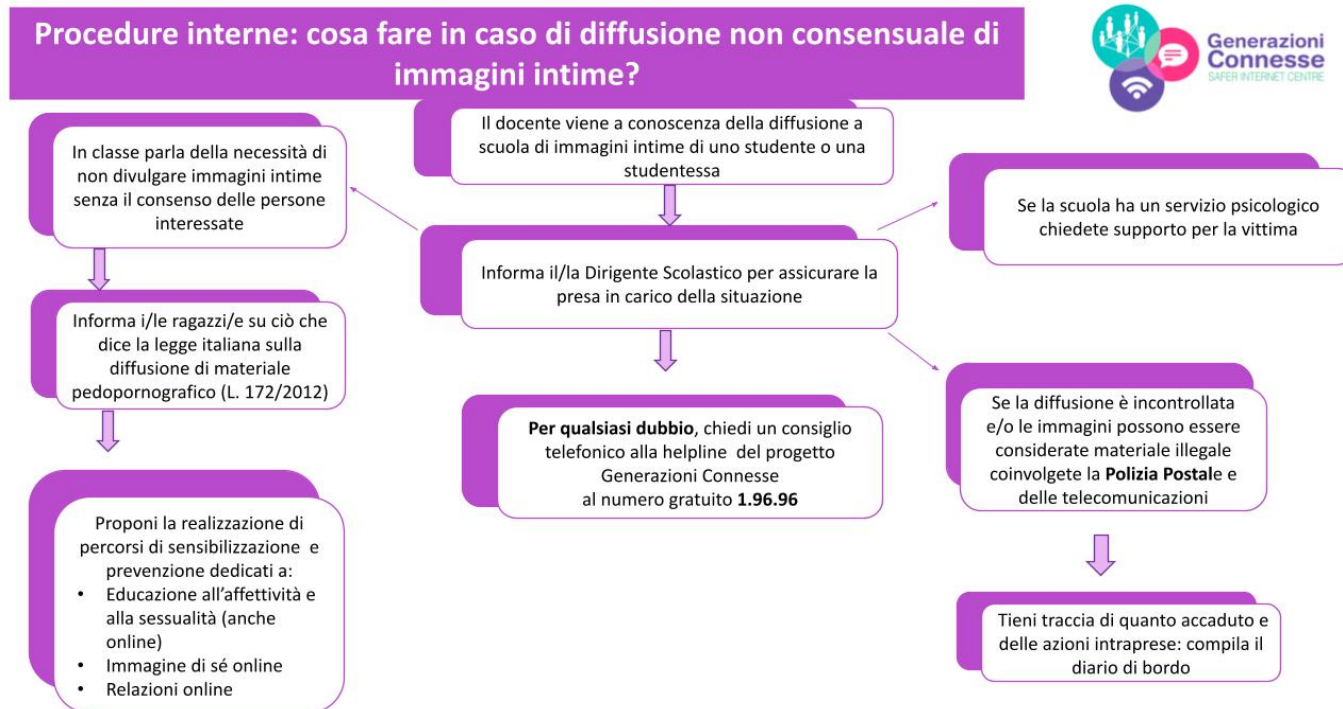


Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



Procedure interne: cosa fare in caso di Adescamento Online?





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, l'Istituto prevede alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- email del Dirigente Scolastico scuola@istvas.edu.it o dei referenti Bullismo/ Cyberbullismo;
- sportello di ascolto CIC;
- progetti specifici (psicologo scolastico) e sportello di ascolto relativo;

Per ogni altra indicazione si fa riferimento alla sezione specifica istituzionale del sito web di Istituto "PREVENZIONE AL BULLISMO E CYBERBULLISMO" disponibile al seguente link: <https://istvas.edu.it/prevenzione-al-bullismo-ed-al-cyberbullismo/>.



MIM

Ministero dell'Istruzione
e del Merito



Attestato di

SCUOLA VIRTUOSA

VANVITELLI - STRACCA - ANGELINI

**Istituzione Scolastica dotata del documento di eSafety
per la tutela dei minori in rete**

Realizzato in data - 16/01/2026 - 10:48



**Generazioni
Connesse**
SAFER INTERNET CENTRE



**Co-funded by
the European Union**