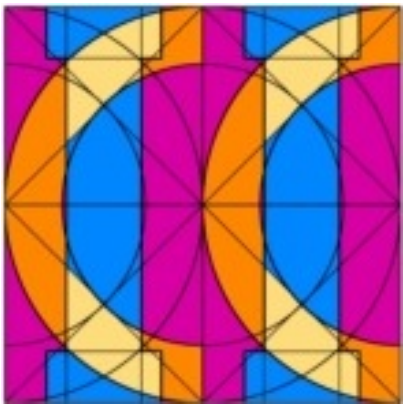


Documento di ePolicy
ITALO CALVINO - GALLIATE

LARGO PIAVE 4 - 28066 - GALLIATE
Novara (NO) - Piemonte
Data di approvazione: 23/10/2024 - 18:40

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

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.

Attraverso l'epolicy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alle tecnologie che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di internet.

L'ePolicy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC (Tecnologie dell'Informazione e della Comunicazione) o ICT (Information and Comunication Tecnoligies).

Le TIC rivestono un ruolo di grande importanza nel processo educativo e di apprendimento degli studenti e delle studentesse. Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

L'ePolicy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali. Nello specifico:

● l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;

● le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione in ambiente scolastico;

● le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;

● le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

Si sottolinea l'aspetto dinamico di questo documento, che si concretizzerà nel suo continuo aggiornamento in risposta ad eventuali future esigenze legate all'uso corretto e consapevole delle TIC

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

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

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

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

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

IL DIRIGENTE SCOLASTICO

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

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

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

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

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

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

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

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

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

Il Team ha il compito di:

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

I/LE DOCENTI

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

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

RESPONSABILE DELLA PROTEZIONE DEI DATI

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

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

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

GLI STUDENTI E LE STUDENTESSE

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

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

I GENITORI/ADULTI DI RIFERIMENTO

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

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

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

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

A integrazione di quanto sopra indicato l'I.C. sottoscrive i seguenti estratti dal DM 18/2021 allegato "Linee di orientamento per la prevenzione e il contrasto dei fenomeni di Bullismo e Cyberbullismo", Tabella 2 "Raccomandazioni e responsabilità degli organi e del personale della scuola".

Dirigente scolastico

Elabora, in collaborazione con il/i referente/i per il bullismo e il cyberbullismo, nell'ambito dell' autonomia delproprio istituto, un Regolamento condiviso per il contrasto dei fenomeni di bullismo e cyberbullismo, che preveda sanzioni in un'ottica di giustizia riparativa e forme di supporto alle vittime. Il Regolamento deve essere esplicitato nel Patto di corresponsabilità educativa firmato dai genitori. I contenuti del Regolamento vanno condivisi e approvati dal Consiglio d'istituto.

Organizza e coordina i Team Antibullismo e per l'Emergenza.

Predispone eventuali piani di sorveglianza in funzione delle necessità della scuola.

Consiglio d'Istituto

Approva il Regolamento d'istituto, che deve contenere possibili azioni sanzionatorie e/o riparative in caso di bullismo e cyberbullismo.

Facilita la promozione del Patto di corresponsabilità tra scuola e famiglia.

Collegio dei Docenti

All'interno del PTOF e del Patto di corresponsabilità *propone* azioni e attività per la prevenzione dei fenomeni di bullismo e cyberbullismo, comprensive delle azioni di prevenzione primaria/universale specifiche per ogni ordine di scuola e delle azioni indicate rivolte a prendere in carico le situazioni di emergenza nella scuola. In modo particolare, *propone* attività di formazione rivolte agli studenti sulle tematiche di bullismo, cyberbullismo ed educazione digitale.

In relazione alle situazioni di emergenza, approva i protocolli di segnalazione e intervento promossi dal Team Antibullismo della scuola e collabora attivamente con il Team e le altre agenzie per la soluzione dei problemi.

Predispone gli obiettivi nell'area educativa, per prevenire e contrastare il bullismo e il cyberbullismo attraverso attività di curriculum scolastico. In tal senso, è importante legare la progettazione della scuola in una ottica di prevenzione dei fenomeni di bullismo e cyberbullismo riferendosi a quanto previsto con il DM 07/09/2024 n.18 "Linee guida per l'insegnamento dell'educazione civica".

Partecipa alle attività di formazione per il contrasto dei fenomeni di bullismo e cyberbullismo organizzate da ogni autonomia scolastica, eventualmente avvalendosi di attività offerte da servizi istituzionali o enti qualificati presenti sul territorio.

I **Coordinatori dei Consigli di classe**

Monitorano che vengano misurati gli obiettivi dell'area educativa, attivando le procedure anti bullismo.

Registrano nei verbali del Consiglio di classe: casi di bullismo, comminazione delle sanzioni deliberate, attività di recupero, collaborazioni con pedagogista, psicologo, forze dell'ordine specializzate nell'intervento per il bullismo e il cyberbullismo, enti del territorio in rete (con riferimento e coordinamento eventuale da parte delle prefetture).

I **collaboratori scolastici** e gli **assistenti tecnici**

Svolgono un ruolo di vigilanza attiva nelle aree dove si svolgono gli intervalli, nelle mense, negli spogliatoi delle palestre, negli spazi esterni, al cambio dell'ora di lezione e durante i viaggi di istruzione, ferme restando le responsabilità dei docenti.

Partecipano alle attività di formazione per il bullismo e il cyberbullismo organizzate dalla scuola.

Se dovessero intervenire per bloccare eventuali comportamenti di bullismo in essere, lo faranno applicando le modalità previste dal Regolamento d'Istituto.

Il **Referente d'Istituto per l'ePolicy**

Si rimanda ai contenuti dei parr. 1.4, 1.5, 3.1, 3.2.

Il **Referente scolastico area bullismo e cyberbullismo** (detto **Referente contro il (cyber)bullismo**)

Collabora con gli insegnanti della scuola, propone corsi di formazione al Collegio dei docenti, coadiuva il Dirigente scolastico nella redazione dei Piani di vigilanza attiva ai fini della prevenzione degli episodi di bullismo e di cyberbullismo, monitora i casi di bullismo e cyberbullismo, coordina i Team Antibullismo e per l'Emergenza, crea alleanze con il Referente territoriale e regionale, coinvolge in un'azione di collaborazione Enti del territorio in rete (psicologi, forze dell'ordine, assistenti sociali, pedagogisti, ecc.).

Descrizione dettagliata dei compiti del Referente contro il (cyber)bullismo è contenuta nei parr. 1.4, 1.5 e 4.2.

Il **Team antibullismo e per l'emergenza**

Comunicano al Referente regionale (anche tramite i Referenti territoriali), alla fine di ogni anno scolastico, i casi di bullismo o cyberbullismo.

E' costituito dal Dirigente scolastico, dal Referente per la legalità/ contro il (cyber)bullismo, dal Docente coordinatore della classe a cui appartiene la vittima, dall'eventuale docente con cui la vittima si è confidata, dallo psicologo della scuola, se la vittima ha scelto di confidarsi con lui; in "casi acuti", da collaboratori esterni.

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.

- Polizia Municipale di Galliate
- Comando dei Carabinieri di Galliate
- Procura della Repubblica di Novara
- Tribunale per i Minorenni: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.
- 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 danno dovute a situazioni ambientali carenti o inadeguate.
- 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.
- 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.

Gli **studenti** e le **studentesse**

Sono chiamati a essere parte attiva nelle azioni di contrasto al bullismo e al cyberbullismo e di tutela della vittima, riferendo ai docenti e agli altri adulti gli episodi e i comportamenti di bullismo e cyberbullismo di cui vengono a conoscenza e supportando il/la compagno/a vittima (consolandola e intervenendo attivamente in sua difesa).

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.

A integrazione di quanto sopra esposto, si indicano altri documenti in diretta correlazione con l'ePolicy presso il nostro Istituto

1. il *Rapporto di Auto Valutazione* (RAV): è lo strumento che accompagna e documenta la prima fase del procedimento di valutazione delle istituzioni scolastiche, ossia l'autovalutazione. Il RAV fornisce una rappresentazione della scuola attraverso un'analisi del suo funzionamento e costituisce inoltre la base per individuare le priorità e i traguardi verso cui orientare il piano di miglioramento.
2. il *Curricolo digitale d'Istituto*, a sua volta correlato alle indicazioni per l'Educazione civica digitale e alle Linee guida per l'educazione civica (DM 183/2024); cfr. par. 2.2
3. il *Regolamento disciplinare degli alunni* (primaria e secondaria); cfr. par. 3.3

La verifica delle reciproche correlazioni tra ePolicy e i documenti citati è a cura del Referente per l'ePolicy

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

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

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

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

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

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

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

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

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

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

Sul sito istituzionale dell'Istituto Comprensivo verrà caricata la versione integrale dell'ePolicy a cura del **Referente del sito**, ricevuta dal **Referente per l'ePolicy**. L'Istituto ha curato presentazioni (versioni *friendly*) del documento ePolicy per famiglie e collaboratori esterni, per gli alunni della scuola primaria e per gli alunni della scuola secondaria.

Il Referente per l'ePolicy ne dà notizia

- a determinate realtà esterne: al Comune (Assessorato all'istruzione, Servizi sociali, Polizia), al locale Comando dei

Carabinieri, al Consorzio Intercomunale per i Servizi Assistenziali (C.I.S.A.) dell'Ovest Ticino, alla Scuola-Polo locale per la formazione contro bullismo e cyberbullismo, all'Ufficio Scolastico Territoriale (U.S.T.) e all'Ufficio Scolastico Regionale (U.S.R.); a queste realtà se ne possono aggiungere altre, a seconda dei casi che si dovrà gestire e che conseguentemente entreranno a far parte del Team per l'emergenza;

- a tutto il personale scolastico: docente, educativo e - per il tramite del Direttore dei Servizi Generali Amministrativi (D.S.G.A.) - assistente tecnico-amministrativo (A.T.A)
- ai genitori degli alunni o a chi ne esercita la potestà.

I suddetti referenti avranno cura di tenere aggiornati il sito e i destinatari citati sui periodici cambiamenti.

Il **Referente contro il (cyber)bullismo**, in collaborazione con altri docenti, organizzerà le illustrazioni delle più aggiornate presentazioni sintetiche del presente documento per le famiglie e per gli alunni; rispettivamente,

- in occasione dell'open-day ed eventualmente di altre assemblee per i genitori o di chi ne esercita la potestà; ne verrà comunque data informativa tramite apposita circolare;
- durante le prime lezioni dedicate al perseguimento del nucleo concettuale "cittadinanza digitale" delle "Linee guida per l'insegnamento dell'educazione civica" (DM 183/2024 allegato); eventualmente in occasione del Safer Internet Day; ne verrà inoltre richiamata l'esistenza mediante appositi pro-memoria affissi negli ambienti comuni dell'edificio scolastico.

Il contenuto del presente paragrafo risponde alle indicazioni fornite dal documento **UNESCO "Sei pilastri per la trasformazione digitale dell'educazione. Un quadro di riferimento comune", 2024**. Precisamente il pilastro **4 Capacità e Cultura**, componente **4. Relazioni con le comunità locali**. Rafforzare le partnership con le comunità locali è importante sia per fornire risorse educative digitali sia per coinvolgere i membri della comunità nella trasformazione digitale dell'educazione. La partecipazione delle comunità promuove un ambiente di supporto per la trasformazione digitale.

1.5 - I Piani di Azione dell'ePolicy

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

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

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

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

1° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

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

MODULO II

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

MODULO III

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

MODULO IV

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

2° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

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

MODULO II

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

Le indicazioni standard per tutti gli Istituti scolastici della Repubblica aderenti al progetto ePolicy sono state recepite come segue.

PERIODO DI PREPARAZIONE DEL DOCUMENTO ePOLICY: MAGGIO 2023 - OTTOBRE 2024

- maggio 2023, Collegio Docenti Unitario (C.D.U.): presentazione dell'ePolicy e delibera di adozione e svolgimento della proposta progettuale
- novembre 2023, progetto "Per Tommaso" sui temi del (cyber)bullismo, da parte di studentesse e studenti dell'I.I.S. "Pascal" di Romentino (No), con le classi 2° della scuola secondaria ("prevenzione secondaria", a norma del DM 18/2021)
- dicembre 2023, Open Day: spiegazione del progetto ePolicy, adottato con delibera
- gennaio-febbraio 2024: attivazione del progetto "Un patentino per lo smartphone", promosso dall'A.S.L 13 di Novara, tenuto da docenti interni appositamente formati, rivolto alle classi 1° della scuola secondaria, sull'uso consapevole dei dispositivi mobili e sui rischi della rete ("prevenzione secondaria", a norma del DM 18/2021)
- febbraio 2024: partecipazione on-line al Safer Internet Day (S.I.D.), da parte di alcune classi dell'Istituto, a discrezione di rispettivi docenti
- marzo 2024
    - incontro delle classi 3° della scuola secondaria con il Maresciallo del Comando locale dei Carabinieri sulle varie forme cyberbullismo ("prevenzione secondaria", a norma del DM 18/2021)
    - rilevazione delle competenze digitali del personale docente tramite la piattaforma *SelfieforTeachers*
    - comunicazione di specifiche offerte formative del *Safer Internet Center* ai genitori o a chi ne esercita la potestà
- aprile-maggio 2024: compilazione del questionario di autovalutazione e partecipazione al corso di formazione da parte dei membri del Team ePolicy: referenti contro il (cyber)bullismo e animatori digitali dei tre ordini di scuole dell'Istituto
- maggio 2024: compilazione e invio all'U.S.R. del modulo di rilevazione dei casi di bullismo e di cyberbullismo, con riferimento al DM 18/2021
- giugno-agosto 2024: impostazione dei capitoli del documento ePolicy
- settembre 2024: completamento dei capitoli del documento ePolicy e dei relativi allegati previsti, anche alla luce delle nuove "Linee guida per l'insegnamento dell'Educazione civica"(DM 183/2024); conseguente aggiornamento del regolamento disciplinare degli alunni
- ottobre 2024: approvazione, da parte del CDU,
    - del documento ePolicy e dei relativi allegati
    - negli altri documenti dell'Istituto, nei quali l'ePolicy è stato integrato

PRIMO ANNO DI ATTIVITA' CON L'ePOLICY (2023-2024)

- Informativa sul documento ePolicy come illustrato al precedente paragrafo 1.4
- Introduzione del kit didattico come metodo e risorsa di lavoro in alcune classi pilota

SECONDO ANNO DI ATTIVITA' CON L'ePOLICY (2024-2025)

L'istituto utilizza il *kit didattico* come pratica metodologica e risorse a disposizione dei docenti attraverso il sito del *Safer Internet Center*

INIZIATIVE AD ATTIVAZIONE ANNUALE

- Indicazioni dei **Referenti per l'Educazione civica, il curricolo digitale e il (cyber)bullismo** agli altri docenti: aggiornamenti utili alla progettazione didattica per i rispettivi ambiti di competenza
- Indicazione dell'**Animatore digitale** al nuovo personale docente: rilevazione delle personali competenze digitali, tramite la piattaforma *SelfieforTeachers*
- A cura dei **docenti incaricati della Cittadinanza digitale nell'educazione civica**: "Prevenzione primaria" (DM 18/2021), ossia rilevazione dei bisogni e degli interessi degli allievi inerenti alla cittadinanza digitale e conseguente progettazione, avvalendosi anche delle risorse del Safer Internet Center
- A cura del **Referente contro il (cyber)bullismo**:
    - informativa ai genitori, o a chi ne esercita la potestà, delle specifiche offerte formative del *Safer Internet Center* o di altre realtà dello stesso settore
    - informativa al nuovo personale scolastico (docente, educativo, ATA) del documento ePolicy in vigore
    - illustrazione delle presentazioni sintetiche dell'ePolicy - eventualmente aggiornate - per le famiglie e di quelle per gli alunni, come indicato al par. 1.4
    - "Prevenzione secondaria" (DM 18/2021)
        - scuola primaria:
            - classi 4°-5°: incontro con Carabinieri del Comando locale
            - classi 4°-5°: nell'ambito del progetto "Neo connessi Wind3" percorso "Nati digital: storie per piccoli esploratori curiosi" in collaborazione con la Polizia di Stato
        - scuola secondaria: a cura di specifici referenti e di altro personale docente coinvolto
            - classi 1°: progetto "Patentino per lo Smartphone"
            - classi 2°: progetto "Per Tommaso"
            - classi 3°: incontro con Carabinieri del Comando locale
    - **eventualmente** con altri docenti: compilazione del questionario annuale di monitoraggio dei casi di (cyber)bullismo della *Piattaforma Elisa*
    - Trasmissione del diario di bordo, degli eventuali episodi di (cyber)bullismo avvenuti, all'USR, da parte del Referente contro il (cyber)bullismo

INIZIATIVE AD ATTIVAZIONE TRIENNALE, A PARTIRE DALL'A.S. 2025/2026

A cura del **Referente contro il (cyber)bullismo**: rilevazione e conseguente soddisfazione - mediante incontri o corsi con esperti interni o esterni - dei bisogni dei genitori, o di chi ne esercita la potestà - non precedentemente soddisfatti dall'offerta del *Safer Internet Center* - dei rischi su internet in cui possono incorrere i propri figli.

L'aggiornamento verrà organizzato dall'Istituto con il supporto del personale interno e se necessario personale esterno, oltre che col supporto della rete scolastica del territorio (USR, Osservatorio regionale sul bullismo, scuola polo, ecc), delle amministrazioni comunali e dei servizi socio-educativi.

INIZIATIVE AD ATTIVAZIONE TRIENNALE, A PARTIRE DALL'A.S. 2026/2027

A cura dell'**Animatore digitale**:

- raccolta di almeno un attestato (o autocertificazione) per docente, di avvenuto aggiornamento
    - sia sul (cyber)bullismo, soprattutto mediante la *Piattaforma Elisa* e il *Safer Internet Center*
    - sia sulle restanti competenze digitali
- rilevazione dei bisogni dei docenti su questi ambiti

Alla luce degli esiti della raccolta e della rilevazione e a cura dell'Animatore digitale e del **Referente contro il**

(cyber)bullismo: organizzazione di formazione specifica, con riferimento particolare rispettivamente al documento DigCompEDU e alle piattaforme *Elisa* e del *Safer Internet Center*

Quanti non avranno seguito almeno un corso su questi ambiti durante gli anni precedenti, saranno tenuti a seguirlo durante l'anno in corso.

L'aggiornamento verrà organizzato dall'Istituto con il supporto del personale interno e se necessario personale esterno, oltre che col supporto della rete scolastica del territorio (USR, Osservatorio regionale sul bullismo, scuola polo, ecc), delle amministrazioni comunali e dei servizi socio-educativi.

Il contenuto del presente paragrafo risponde alle indicazioni fornite dal documento **UNESCO "Sei pilastri per la trasformazione digitale dell'educazione. Un quadro di riferimento comune", 2024**. Precisamente il pilastro **4 Capacità e Cultura**

- Componente **2. Competenze e mentalità degli insegnanti**. Sviluppare le competenze pedagogiche digitali e ibride degli insegnanti e dei leader educativi è cruciale. Attraverso programmi di formazione iniziale e continua, gli educatori devono essere formati per integrare efficacemente la tecnologia nell'insegnamento, nell'apprendimento e nella gestione scolastica. Questo favorisce l'apertura all'innovazione educativa.
- Componente **3. Ruolo dei genitori e dei caregiver**. Coinvolgere i genitori e i caregiver è essenziale per sostenere l'apprendimento digitale in modo sicuro ed efficace. La loro consapevolezza e preparazione nel supportare comportamenti positivi verso la tecnologia sono fondamentali per promuovere il benessere e il successo degli studenti nel contesto digitale.
- Componente **4. Relazioni con le comunità locali**. Rafforzare le partnership con le comunità locali è importante sia per fornire risorse educative digitali sia per coinvolgere i membri della comunità nella trasformazione digitale dell'educazione. La partecipazione delle comunità promuove un ambiente di supporto per la trasformazione digitale.

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

Il Kit didattico sviluppato da Generazioni Connesse è uno strumento che raccoglie tematiche e contenuti che sono alla base dello sviluppo di una piena cittadinanza digitale degli studenti e delle studentesse. Il kit è composto da percorsi educativi che guidano i docenti nella realizzazione di percorsi laboratoriali di educazione civica digitale da proporre nelle proprie classi. Questi materiali si basano sul metodo scientifico EAS (episodi di apprendimento situato) che si intreccia col DigComp 2.2 (quadro di riferimento delle competenze digitali dei cittadini e gli otto livelli di padronanza).

Il Kit Didattico è organizzato in cinque aree:

1. La prima parte è legata a una generale comprensione del cambiamento originato dalla convergenza tra tecnologie digitali e connettività.
2. La seconda parte, associata all'educazione ai media, è invece rivolta a chiarire le profonde implicazioni che i cambiamenti originati dalle tecnologie digitali hanno sulla nostra dimensione individuale e sociale.
3. La terza parte affronta l'educazione all'informazione (information literacy), sia attraverso lo sviluppo delle competenze necessarie alla ricerca, raccolta, utilizzo e conservazione di informazioni, che attraverso la comprensione delle dinamiche legate al profondo cambiamento in atto nell'ecosistema della produzione e distribuzione di informazione.
4. La quarta parte affronta invece le implicazioni della quantificazione e della computazione, dinamiche intrinsecamente legate alla diffusione delle tecnologie digitali.
5. La quinta parte sviluppa infine la connessione tra cittadinanza e creatività digitale.

Al seguente link è possibile scaricare una breve descrizione del metodo EAS e la sua integrazione col DigComp 2.2

https://www.generazioniconnesse.it/_file/documenti/ECD/ECD-2022/Cornice%20Metodologica_Kit_2023.pdf

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.

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

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

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

Gli strumenti da adottare per poter ridurre l'incidenza di situazioni di rischio si configurano come interventi di **sensibilizzazione e prevenzione**

- Nel caso della sensibilizzazione si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento: l'intervento è volto a fornire le informazioni necessarie per riconoscere il fenomeno, ma anche illustrare possibili soluzioni e\o i comportamenti da seguire

Per perseguire questo obiettivo, il nostro Istituto organizza ogni anno almeno un incontro con le forze dell'Ordine rivolto prevalentemente agli alunni delle classi terze della SSPG; per le seconde è oramai consolidato il coinvolgimento delle seconde nel Progetto per Tommaso (Peer education) mentre le classi prime sono coinvolte nel percorso di formazione Un Patentino per lo smartphone.

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

In tal senso la nostra scuola ha redatto un curricolo per l'educazione digitale che prevede azioni volte ad accompagnare i

ragazzi nel processo di approccio al mondo digitale in maniera consapevole e responsabile.

2.2 - Il Curricolo Digitale

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

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

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

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

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

I ragazzi usano la rete quotidianamente, talvolta in modo intuitivo; ma non per questo possiamo affermare che più degli adulti siano dotati di migliori competenze digitali. Infatti, la competenza digitale presuppone l'interesse per le relative tecnologie e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere e lavorare.

Per tali ragioni, l'Istituto ha redatto **tre curricoli digitali**: uno per la scuola d'infanzia, uno per la scuola primaria, uno per la scuola secondaria.

Tutti i curricoli sono stati redatti assumendo come primo riferimento le competenze elencate nel documento **DigComp 2.2**.

Rispettando un criterio di affinità, alcune sono state correlate

- con le cinque parti del documento sull'**Educazione civica digitale** proposto dal *Safer Internet Center*;
- con le **Linee guida per l'insegnamento dell'educazione civica (DM 183/2024 allegato)**; precisamente,
    - con una tra le competenze per la scuola d'infanzia;
    - con i traguardi per lo sviluppo delle competenze per il primo ciclo di istruzione e con gli obiettivi di apprendimento per la scuola primaria e per la scuola secondaria di primo grado, inerenti al nucleo concettuale "**cittadinanza digitale**".

Rispettando un criterio di contitolarità, tutte sono state correlate

- a precisi campi d'esperienza, per la scuola d'infanzia
- al curricolo di tecnologia, per la scuola primaria
- a tutte le discipline, con attenzione prevalente a tecnologia, per la scuola secondaria di primo grado

Ulteriori aspetti della progettazione sui curricoli digitali vengono definiti all'inizio di ogni anno scolastico, in concomitanza con quelli della progettazione sui curricoli di **Educazione civica**.

La nostra scuola si impegna ad effettuare ciclicamente una **rilevazione** dei **bisogni** di aggiornamento e a promuovere percorsi formativi su tali temi (cfr. par. 1.5).

Per quanto affermato, i curricoli digitali dell'Istituto rispondono alle indicazioni fornite dal documento **UNESCO, *Sei pilastri per la trasformazione digitale dell'educazione. Un quadro di riferimento comune*, 2024**. Precisamente

- pilastro 4 *Capacità e cultura*
  - componente 1 *Competenze per il futuro,*
  - componente 5 *Innovazione e generazione di conoscenze*;
- pilastro 5 *Contenuti e soluzioni*
  - componente 3 *Allineamento curriculare*,
  - compentente 5 *Valutazione e certificazione*;
- pilastro 6 *Dati e prove*, componente 5 *Intelligenza Artificiale (IA)*.

Ciascun curricolo digitale ha un proprio **referente**, che deve supervisionare l'attuazione del curricolo e che deve perciò confrontarsi anzitutto con l'**Animatore digitale** e con i **Referenti di Educazione civica**.

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.

Il *Safer Internet Center* è co-finanziato dalla Commissione Europea nell'ambito del programma *Digital Europe* e fa parte di una di una rete che si concretizza in una piattaforma online dal nome *Better Internet for Kids* gestita da *European Schoolnet* in collaborazione con INSAFE che accorpa tutti i SIC europei, e INHOPE un network che accorpa tutte le hotlines europee.

Il Kit didattico, offerto dal *Safer Internet Center*,

1. utilizza la **metodologia EAS** - Episodi di Apprendimento Situato - sviluppata dal CREMIT in grado di al docente offrire un quadro metodologico efficace ed operativo per costruire una lezione che comprenda al suo interno le diverse dimensioni utili all'apprendimento: problem setting, learning by doing e learning by reflecting;
2. è disegnato sul **framework** europeo di riferimento per le competenze digitali **DigComp 2.2** ed in questo modo il docente, nello svolgimento della singola lezione, è in grado di connettere l'attività con il curricolo verticale del proprio Istituto e con le indicazioni sull'educazione civica digitale che utilizzano lo stesso riferimento;
3. propone anche **contenuti dedicati ai docenti di sostegno** progettati sulla base degli indicatori ICF (classificazione internazionale del funzionamento, della disabilità e della salute è un sistema di classificazione della disabilità sviluppata dall'Organizzazione mondiale della Sanità) e collegando questi ultimi agli indicatori di competenza di

ciascuna attività. In questo modo il docente di sostegno può realizzare le attività personalizzandole sull'allievo e proponendo strategie di apprendimento funzionali anche alla partecipazione, con la classe, alle attività;

4. contiene **risorse digitali** che spaziano dall'uso di immagini digitalizzate a percorsi didattici completi; e trattano tematiche che vanno da DEEP FAKE, WEB REPUTATION, BODY SHAMING, ZOOMBOMBING, ADESCAMENTO ONLINE, NETIQUETTE, SHARENTING, DIPENDENZA DALLA RETE, a molte altre.

Alcune risorse sono già state utilizzate dal nostro Istituto nell'ambito di vari progetti come il *Patentino per lo smartphone* e in occasione del *Safer Internet Day*; ma il nostro impegno consiste nell'implementare l'uso del kit didattico in un'ottica di sempre maggiore attenzione ai pericoli ai quali sono esposti i nostri alunni per aiutarli a navigare in un mare pieno di insidie col giusto salvagente.

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.

Ogni giorno a scuola vengono trattati numerosi dati personali che riguardano sia il personale scolastico, sia gli alunni con le rispettive famiglie. Certe volte, tali dati possono riguardare informazioni sensibili, come problemi di salute o disagi psico-sociali. Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, in particolar modo quando i soggetti coinvolti sono minorenni.

Per tale ragione, l'Istituto si è dotato dei seguenti documenti:

- *Documento delle Misure a Tutela dei Dati delle Persone (DMTDP) redatto ai sensi e per gli effetti degli artt 24 comma 1, 30 e 35 del Regolamento dell'Unione Europea 2016/279*. Esso è stato elaborato in data 22/03/2024 secondo il modello rev. 1-2021; e contiene:
  - il *Registro delle attività di trattamento* (art. 30 GDPR)
  - la *Valutazione d'impatto* (art. 35 GDPR)
- *Guida alla procedura* ***Data Brench*** *per il Titolare del trattamento* (secondo il modello rev 1.1), in "aderenza ai principi e alle disposizioni contenute nel Regolamento UE 679/2016 (Considerando n. 85,86,87,88 ed Artt. 33 e 34) e nella *Guidelines on personal data breach notification under Regulation 2016/679 – article 29 data protection working party*"; da attuare in caso di violazione dei dati (hacker e altro)
- **Informative sul trattamento dei dati personali ai sensi dell'art.13 del Regolamento UE 2016/679**. Queste vengono fornite
  - al momento dell'iscrizione degli allievi, ai rispettivi genitori (o a chi ne esercita la potestà)
  - sul **Diario scolastico**, annualmente consegnato ad allievi e genitori delle Scuole primaria e secondaria di primo grado; particolare attenzione viene prestata alla normativa sulla diffusione di immagini, video e materiale multimediale; e sulla trasmissione di documenti e certificazioni sanitarie;
  - al momento della sottoscrizione del **contratto di lavoro e/o d'incarico** (cfr. *Registro delle attività di*

trattamento). Vengono fornite, su supporto cartaceo, istruzioni particolareggiate nei limiti delle operazioni di trattamento e delle categorie di dati, necessarie ai fini dello svolgimento della propria funzione - e ciclicamente la scuola organizza corsi di aggiornamento a riguardo -

- a tutto il **personale scolastico**; in particolare, agli **autorizzati al trattamento**: soggetti interni (dipendenti e assimilati) che trattano dati in nome e per conto del titolare
- ai **responsabili del trattamento**: soggetti esterni che trattano dati in nome e per conto del Titolare, con loro organizzazione autonoma in forza di un contratto.

Nel **Diario scolastico** sono contenuti i moduli per il rilascio delle autorizzazioni all'utilizzo e alla diffusione di immagini e le riprese audio e\o videoriprese realizzate dalla Scuola. Esse, come anche gli elaborati prodotti dagli studenti durante le attività scolastiche, potranno essere utilizzati esclusivamente per documentare e divulgare le attività della Scuola. Non ne è consentito altro uso in contesti o per fini diversi da quelli sopra indicati.

Il **Titolare del trattamento dei dati** è l'Istituto Comprensivo "Italo Calvino" di Galliate (NO) nella persona del proprio rappresentante legale: la Dirigente scolastica, Paola Maria Ferraris.

Il **Responsabile della protezione dei dati** (**RPD** o **DPO**) è lo "Studio Tecnico Legale *Corbellini*", AG.I.COM S.r.l. unipersonale, via XXV Aprile, 12 -20070 San Zenone sul Lambro (MI); Tel 02-90691324; Fax: 02-700527180; Sito web: www.agicomstudio.it

Il contenuto del presente paragrafo risponde alle indicazioni fornite dal documento **UNESCO, *Sei pilastri per la trasformazione digitale dell'educazione. Un quadro di riferimento comune*, 2024**. Precisamente, il pilastro **6 Dati e prove**,

- componente **2 Integrazione del sistema**. I vari sistemi di dati all'interno e all'esterno del settore educativo devono essere interconnessi e interoperabili, consentendo flussi di dati sicuri e continui per supportare i servizi digitali educativi. L'integrazione dei dati permette una visione completa del panorama educativo, migliorando l'efficienza operativa e la qualità delle decisioni.
- componente **3 Qualità e copertura dei dati**. È fondamentale implementare metodologie standardizzate per garantire che i dati raccolti siano accurati, affidabili e completi. Solo con dati di alta qualità è possibile generare intuizioni utili per il miglioramento del sistema educativo.
- componente **4 Sicurezza e privacy**. Sono necessarie misure rigorose per proteggere i dati da accessi non autorizzati e violazioni, garantendo la privacy degli utenti. La protezione dei dati costruisce la fiducia tra gli stakeholder e assicura la conformità agli standard legali ed etici.

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.

P.U.A. è l'acronimo di "**Politica di Uso Accettabile**". È indicata dalla circolare regionale (CR) 142/2003 dell'Ufficio Scolastico Regionale (USR) del Piemonte e si riferisce alla "Politica d'Uso Accettabile e Sicura della Scuola esemplare", proposta dall'*European Schoolnet*. Integrava il *Documento Programmatico per la Sicurezza* (DPS), fino alla successiva abrogazione di quest'ultimo.

Il P.U.A. d'Istituto si compone

- a livello normativo
  - dal "Regolamento sull'uso corretto dei *device* per il personale scolastico e gli allievi"
  - dalle "Indicazioni sull'uso dei *device* per l'animatore digitale"
  - dal "Regolamento disciplinare degli alunni", particolarmente dalle voci su telefoni o device di altro tipo
- a livello formativo
  - dal **Curricolo digitale d'Istituto**, particolarmente le competenze delle aree 2 ("Comunicazione e collaborazione") e 4 ("Sicurezza") del documento dell'Unione Europea (UE) DigComp 2.2
  - dalle iniziative dei livelli di **prevenzione primaria e secondaria**, a norma del **DM 18/2021** e di aggiornamento del personale docente, specificate al n.1.5 del presente documento.

Regolamento sull'uso corretto dei *device* per personale scolastico e allievi

- 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 e lesivo, etc.
- Gli utenti non devono lasciare incustoditi i dispositivi informatici e devono provvedere alla disconnessione del proprio account al termine dell'utilizzo
- 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.)
- I docenti sono responsabili dell'utilizzo dei dispositivi informatici e hanno l'obbligo di sorvegliare e responsabilizzare gli studenti e le studentesse rispetto ad un uso consapevole e sicuro

Indicazioni sull'uso dei *device* per l'animatore digitale

- Accesso al Wi-Fi. Nel caso in cui i dispositivi in dotazione all'istituto abbiano accesso alla rete WiFi, sarà necessario dotarli di credenziali per l'accesso alla rete. Tali credenziali devono essere gestite con la massima cautela e riservatezza
- Utilizzo degli strumenti di didattica digitale. L'accesso alle piattaforme didattiche dell'istituto deve essere consentito esclusivamente previa autenticazione informatica. A ciascun utente devono essere fornite credenziali univoche, che

devono essere custodite con la dovuta diligenza.

ALLEGATO 1 al presente documento: estratti dal Regolamento disciplinare degli alunni, relativi all'utilizzo dei *device*.

Riconducibili alla P.U.A. risultano anche le seguenti disposizioni.

- Il sito dell'Istituto Comprensivo è raggiungibile all'indirizzo www.calvinogalliate.edu.it. La gestione del sito della scuola e la rispondenza alle normative, per quanto concerne i contenuti (accuratezza, appropriatezza e aggiornamento) e le tecniche di realizzazione e progettazione, sono a cura dell'**Animatore digitale** e del **Referente del sito *web***, sotto la supervisione della **Dirigente scolastica** in qualità di Responsabile del trattamento dei dati. Sul sito, costantemente aggiornato, è possibile trovare i documenti citati nel parr. nn. 1.3, 2.2, 3.2, 4.2.
- Gli indirizzi email dell'Istituto comprensivo, del personale scolastico e degli alunni presentano il dominio **@calvinogalliate.edu.it** e sono protetti da antivirus e antispam. Gli indirizzi email privati del personale scolastico non vengono pubblicati, nè condivisi con alunni e famiglie.
- Per le **comunicazioni** tra **docenti**, **alunni** e **famiglie** degli alunni vengono utilizzati
  - i suddetti indirizzi e-mail istituzionali,
  - la piattaforma **GSuite**, in particolare **Google Classroom**,
  - il **registro elettronico**, appoggiato alla piattaforma *web* AXIOS, a cui si accede tramite gli account scolastici.

L'Istituto possiede un proprio **profilo** sull'applicazione social **Instagram**, con cui pubblicizza le proprie attivita e a cura del **Referente del sito *web***

Il contenuto del presente paragrafo risponde alle indicazioni fornite dal documento ***UNESCO "Sei pilastri per la trasformazione digitale dell'educazione. Un quadro di riferimento comune", 2024***. Precisamente il pilastro **4 Contenuti e soluzioni**

- componente **1. Piattaforme di apprendimento**: Le piattaforme digitali devono essere utilizzate per sviluppare, condividere e gestire i contenuti educativi in modo efficace e inclusivo. Devono inoltre essere sicure, garantire la privacy e promuovere l'equità, monitorando l'impatto sull'accesso e sui risultati educativi. Queste piattaforme facilitano l'apprendimento personalizzato e adattivo, favorendo l'interazione tra insegnanti e studenti.
- componente **2. Qualità e apertura del *software* applicativo**: Le applicazioni educative devono essere di alta qualità, facilmente accessibili e aperte, cioè adattabili, liberamente utilizzabili e riutilizzabili. Ciò contribuisce a promuovere l'accesso equo all'istruzione e a supportare diversi stili e bisogni di apprendimento.

3.3 - BYOD

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

"BYOD" è acronimo per "Bring Your Own Device" e si riferisce alla formazione degli alunni su un uso responsabile dei device personali.

I dispositivi tecnologici sono parte integrande della vita personale di ciascuno, compresa quella degli\lle studenti\esse e dei

Docenti, oltre a tutte le figure professionali che, a vario titolo, entrano in contatto con la realtà scolastica, e influenzano necessariamente la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche: fra queste il progetto Generazioni Connesse e il più ampio PNSD.

L'utilizzo dei dispositivi personali da parte degli alunni durante qualsiasi tipo di attività didattica è disciplinato dalla Nota Prot. 5274/2024 “Disposizioni in merito all'uso degli smartphone e del registro elettronico nel primo ciclo d'istruzione - A.S. 2024/2025: “(...) Alla luce delle considerazioni che precedono, a tutela del corretto sviluppo della persona e degli apprendimenti, si dispone il divieto di utilizzo in classe del telefono cellulare, anche a fini educativi e didattici, per gli alunni dalla scuola d'infanzia fino alla secondaria di primo grado, salvo i casi in cui lo stesso sia previsto dal Piano educativo individualizzato o dal Piano didattico personalizzato, come supporto rispettivamente agli alunni con disabilità o con disturbi specifici di apprendimento ovvero per documentate e oggettive condizioni personali (...)”.

Ogni altro aspetto sull'utilizzo dei dispositivi personali da parte degli alunni è disciplinato da quanto affermato nel precedente n. 3.2, anche in considerazione 10 punti del Miur per l'uso dei dispositivi mobili a scuola https://www.miur.gov.it/documents/20182/0/Decalogo+device/da47f30b-aa66-4ab4-ab35-4e01a3fdceed

Il monitoraggio della normativa sull'argomento è a cura dell'**Animatore digitale**

Cap 4 - Segnalazione e gestione dei casi

4.1 - Cosa Segnalare

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

Le procedure indicate nel presente documento (cfr. Cap 4.2) si fanno carico anche dei casi di bullismo e di qualsiasi illecito che possa essere compiuto da un maggiorenne a danno di minorenni, oltre a quelli sopra menzionati. Infatti l'Istituto scolastico deve assicurare la vigilanza all'interno dell'edificio, sia nelle aule, sia in altri spazi, quali corridoi, palestre, spogliatoi, bagni. Si può riscontrare la *culpa in organizzando* della scuola nel caso in cui non siano attuate misure di prevenzione del (cyber)bullismo. La scuola pubblica che invece ha una responsabilità diretta nei riguardi del Ministero dell'Istruzione e del Merito (MIM) della pubblica istruzione quale potrà esercitare l'azione di rivalsa sul docente nell'ipotesi di dolo o colpa grave.

4.2 - Quali strumenti e a chi

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

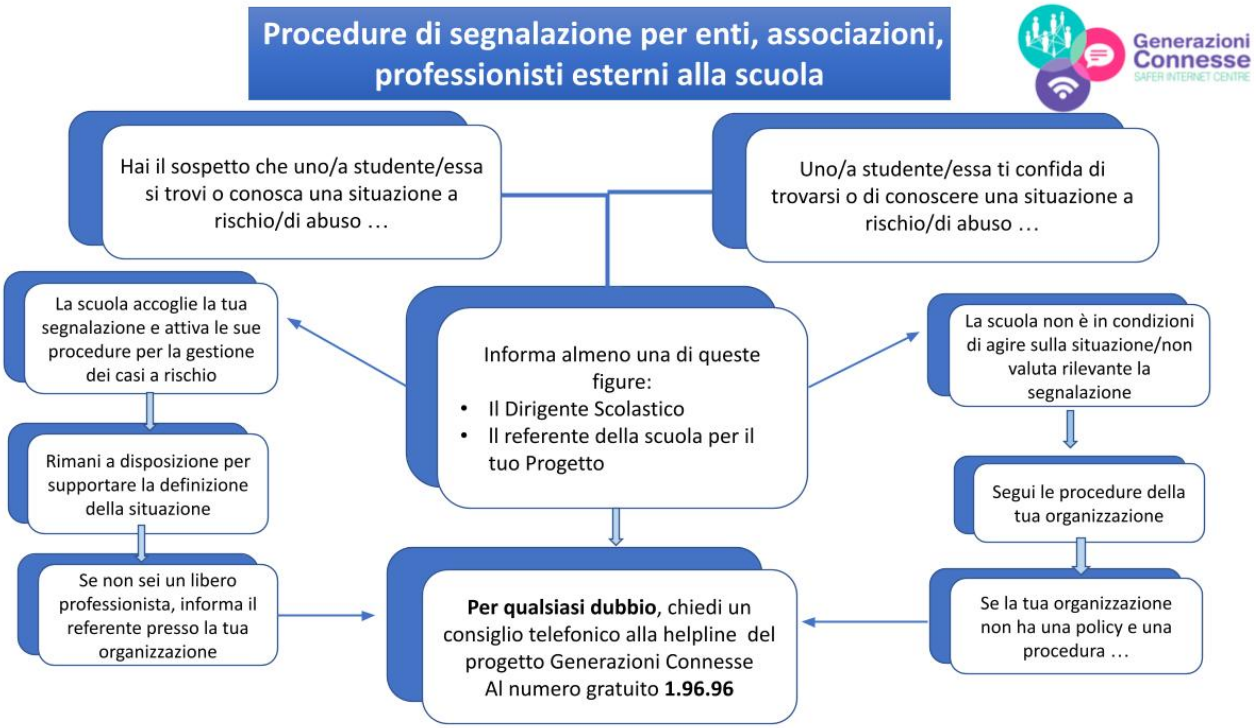
Strumenti a disposizione di studenti/esse

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

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

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

Procedure



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

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

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

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

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

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

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo

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

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

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

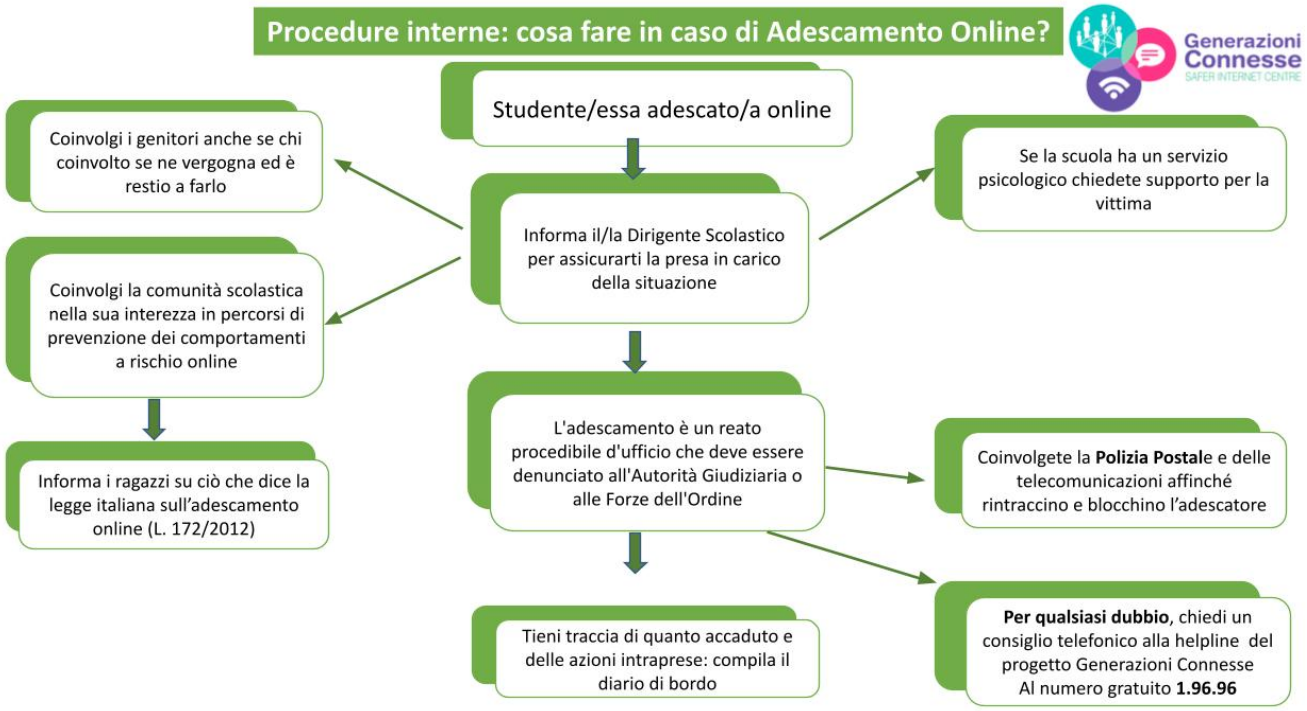
Se emergono evidenze passa allo schema successivo

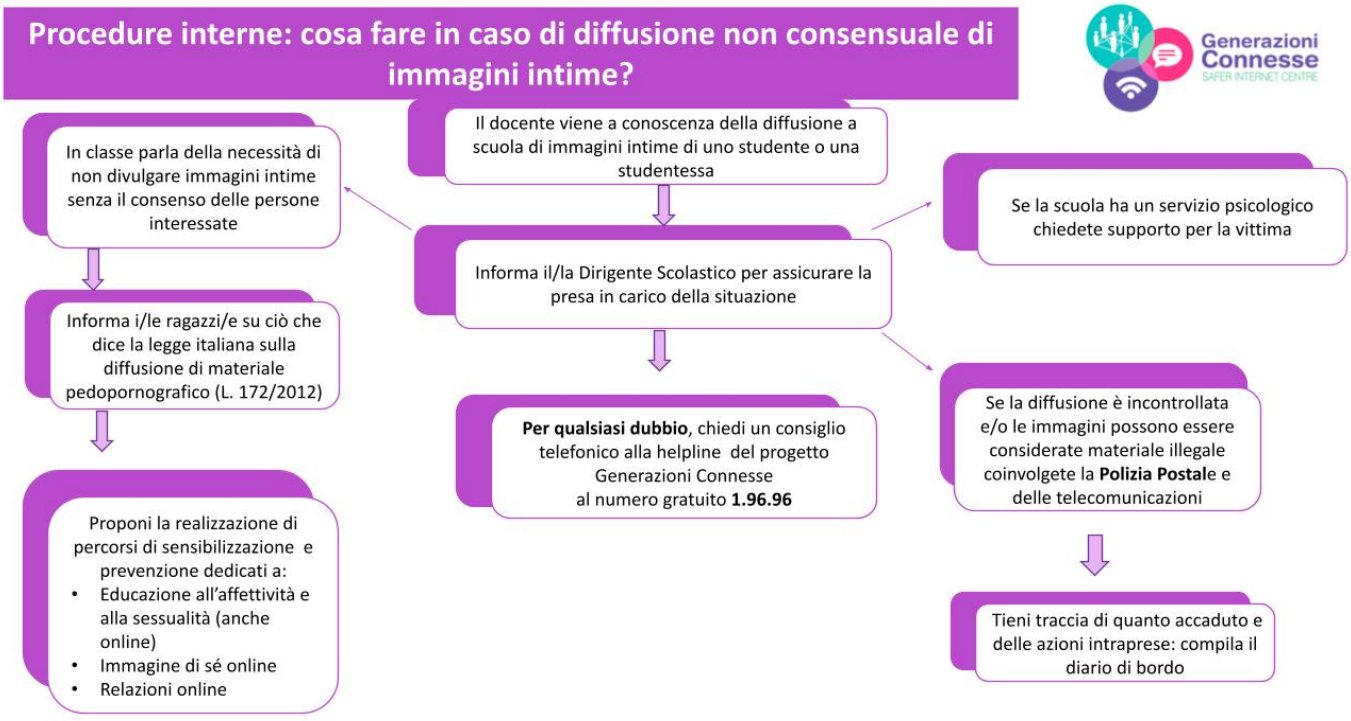
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

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

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

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





L'Istituto ha adottato una specifica procedura da seguire nei casi di (sospetto) (cyber)bullismo e di illecito di maggiorenne verso minorenne (si veda **ALLEGATO 2**).

ALLEGATO 1
Estratti dal Regolamento disciplinare degli alunni, relativi all'utilizzo dei *device per la Scuola Secondaria*

DOVERI	MANCANZE	SANZIONI E AZIONI DI RESPONSABILIZZAZIONE	ORGANO COMPETENTE	PROCEDURA
Osservanza delle disposizioni organizzative riguardanti l'uso del cellulare e di altri dispositivi elettronici (di seguito, denominati *device*)	*Device* personale rimasto acceso, ma comunicato spontaneamente dall'allievo	Richiamo verbale	Docente	Richiamo
	Device personale rimasto acceso	Nota disciplinare sul registro elettronico (livello 2)	Docente	Scrittura della nota
	Uso dei *Device*, propri o altrui, senza comunicazioni con terzi, eventualmente con scatti di fotografie e/o registrazioni di video e/o audio aventi per oggetto solo se stessi	Nota disciplinare sul registro elettronico (livello 3) e assegnazione di compito sull'utilizzo corretto del cellulare, da valutarsi per Educazione civica		Scrittura della nota, assegnazione e valutazione dell'attività indicata
		Convocazione della famiglia	Coordinatore di classe	Convocazione
	Uso dei *Device*, propri o altrui con comunicazioni con terzi, e/o scatto di fotografie e/o registrazione di video e/o audio aventi per oggetto terzi chiaramente identificabili e/o relativa condivisione Accesso al registro elettronico e/o agli account con dominio @calvinogalliate.edu.it NON personali, CON eventuale modifica dei dati e/o diffusione degli stessi	Nota disciplinare sul registro elettronico (livello 4). **Uno o due** giorni di sospensione dalle attività didattiche con obbligo di frequenza e compito da valutare per educazione e civica.	Consiglio di classe	Convocazione del consiglio di classe e dei genitori -o di chi ne esercita la potestà - del responsabile
		Esclusione da iniziative didattiche, fuori dagli edifici scolastici, se non viene manifestato un ravvedimento operoso		
	Utilizzo di *Device* senza l'autorizzazione del docente, in particolare, se è in dotazione alla scuola e se l'allievo l'ha utilizzato per 1. collegare dispositivi esterni 2. installare e/o disinstallare programmi	Sanzione prevista dal documento ePolicy	Referente contro il cyberbullismo	Procedura prevista dal documento ePolicy

	e/o modificarne le impostazioni 3. 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 e/o lesivo di terzi, etc.			
Uso del cellulare e di altri dispositivi elettronici durante visite, uscite e viaggi di istruzione	Divieto dell'uso del telefono o di altri device durante le attività programmate (eccezioni: viaggio in pullman, pausa pranzo)	Nota disciplinare sul registro elettronico (livello 3) e assegnazione di un compito (da valutare) di educazione civica	Docenti accompagnatori	Applicazione della sanzione a partire dal giorno successivo all'attività
	Durante le uscite didattiche e i viaggi di istruzione valgono le stesse norme indicate nel vigente regolamento di disciplina alunni con le seguenti precisazioni: 1. quanto vale per il rapporto con il personale scolastico si intende esteso al personale dei luoghi oggetto dell'uscita/viaggio e di ogni persona incontrata lungo il tragitto; 2. quanto vale per l'utilizzo delle attrezzature scolastiche si intende esteso all'utilizzo e al tocco, anche involontario e istantaneo, del materiale dei luoghi oggetto di visita/viaggio, e di qualsiasi altro materiale lungo il tragitto; 3. le sanzioni previste sono passibili di ulteriori aggravi, mediante delibera del consiglio di classe a seguito di infrazioni, dato che il setting risulta meno strutturato di quello scolastico e perciò caratterizzato da un margine di rischio più alto"			

ALLEGATO 2

Procedura da seguire nei casi di (sospetto) (cyber)bullismo e di illecito di maggiorenne verso minorenne.

Caso SOSPETTO di (cyber)bullismo, o di sospetto illecito di maggiorenne verso minorenne: anzitutto, adescamento (on line) e condivisione (on line) di immagini di minorenni con corpo prevalentemente scoperto o con parti intime scoperte o in pose sessualmente esplicite
1 Il **dipendente**/l'**alunno** della scuola • che sospetta di un episodio di (cyber)bullismo • o di illecito di maggiorenne verso minorenne o a cui un terzo ha comunicato i propri sospetti o le proprie certezze, ma senza fornire prove, avvisa il **Referente contro il (cyber)bullismo** • di persona • o tramite email scolastica
2 Il **Referente contro il (cyber)bullismo** • redige il "Modulo per la segnalazione dei casi" (fornito dal *Safer Internet Center*) • informa i **Coordinatori di classe** delle parti coinvolte e insieme verificano se sussistano i requisiti per la qualificazione del caso come (cyber)bullismo - comprese eventuali note disciplinari registrate. (Possono consultarsi con la *Helpline* di *Generazioni connesse*: Telefono azzurro 1.96.96) Si può parlare di (cyber)bullismo se sono provate intenzionalità, ripetitività, disparità di forze e potere tra i soggetti coinvolti e l'isolamento della vittima. È necessario inoltre capire quello che è il grado di disagio vissuto dallo studente o dalla studentessa
3 In caso di conferma del sospetto, il **Referente contro il (cyber)bullismo** informa il **Dirigente scolastico**. Quest'ultimo, se condivide il sospetto, • invia segnalazione alle Forze dell'ordine mediante modulo di "SEGNALAZIONE di evento o situazione di RISCHIO a Forze di Polizia / Autorità Giudiziaria" (cfr. DM 18/2021, Appendice) • indica ai Coordinatori di classe di invitare i docenti delle parti coinvolte a monitorare la situazione

Caso EVIDENTE di (cyber)bullismo, o di illecito di maggiorenne verso minorenne: anzitutto, adescamento (*on line*) e condivisione (*on line*) di immagini di minorenni con corpo prevalentemente scoperto o con parti intime scoperte o in pose sessualmente esplicite
1 Il **dipendente**/l'**alunno** della scuola che ha avuto prova di un episodio di (cyber)bullismo o di illecito di maggiorenne verso minorenne - o in prima persona o da parte di terzi - avvisa il **Referente contro il (cyber)bullismo** • di persona • o tramite email scolastica e gli consegna le eventuali prove acquisite.

2 Il **Referente contro il (cyber)bullismo**

- compila il "Modulo per la segnalazione dei casi" (fornito dal Safer Internet Center)
- informa i **Coordinatori delle classi** a cui appartengono i minori coinvolti e il **Dirigente scolastico**;
- si confronta con gli stessi Coordinatori per individuare il docente più idoneo ad ascoltare i minori coinvolti; con l'assenso di questi ultimi, avvisa lo psicologo della scuola; l'assenso dei loro genitori, o di chi ne esercita la potestà, va domandato se questi non hanno preventivamente dato il consenso all'accesso del proprio minore allo sportello psicologico della scuola
- (per qualsiasi dubbio, contatta la *Helpline* di *Generazioni connesse*: Telefono Azzurro 1.96.96)

Caso evidente di (cyber)bullismo	***Caso evidente di illecito di maggiorenne verso minorenne***
3 I **Coordinatori delle classi**, a cui appartengono (cyber)bullo e vittima, informano dell'accaduto • i rispettivi genitori, o chi ne esercita la potestà (e li informa che, trattandosi le parti coinvolte di infraquattordicenni, possono chiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi a gestori di siti internet o social - o, successivamente, in caso di non risposta, al Garante per la Privacy) • gli altri docenti delle stesse classi	3 Il **Coordinatore della classe**, a cui appartiene la vittima, informa dell'accaduto gli altri docenti della stessa classe
4 Il **Dirigente scolastico**, il **Referente contro il (cyber)bullismo** e i **genitori della vittima**, accertano se l'atto in questione si configura come reato • in caso affermativo: il Dirigente scolastico invia segnalazione alla Procura dei minori - art. 328 codice penale: omissione in atto d'ufficio • in caso negativo: valutano se inviare segnalazione alle Forze dell'ordine, poi inviata dal Dirigente scolastico con apposito modulo: DM 18/2021 Appendice • provvede alla convocazione del Consiglio della classe a cui appartiene il (cyber)bullo, con eventuali esterni, per valutare quanto previsto dal Regolamento disciplinare	4 Il **Dirigente scolastico** • informa dell'accaduto i genitori della vittima, o chi ne esercita la potestà genitoriale • invia segnalazione alla Procura ordinaria tramite apposito modulo: DM 18/2021 Appendice; art. 328 codice penale: omissione in atto d'ufficio

5 Il **Dirigente scolastico**, in caso di materiale pedopornografico, contatta "Clicca e Segnala" di Telefono Azzurro Italia e STOP_IT di Save the Children Italia

6 I **Docenti della classe a cui appartiene la vittima**, sentiti i suoi genitori e a seconda sia della gravità dell'accaduto, sia della sua risonanza, progettano interventi educativi nella classe (cfr. L.172/2012)
Procedura dettagliata del DM 18/2021, si veda Tabella1: Protocollo di intervento per un primo esame nei casi acuti e di emergenza in calce

7 Il **Referente contro il (cyber)bullismo**, consultandosi con il **Coordinatore di classe**, compila

- il "Modulo per il follow-up dei casi" (fornito dal *Safer Internet Center*)
- il "Diario di bordo" (sul modello dei Moduli del *Safer Internet Center*) da consegnare all'USR entro il termine dell'anno scolastico

TABELLA 1: PROTOCOLLO DI INTERVENTO PER UN PRIMO ESAME NEI CASI ACUTI E DI EMERGENZA

Intervento con la vittima	*Intervento con il bullo*
- accogliere la vittima in un luogo tranquillo e riservato; - mostrare supporto alla vittima e non colpevolizzarla per ciò che è successo; - far comprendere che la scuola è motivata ad aiutare e sostenere la vittima; - informare progressivamente la vittima su ciò che accade di volta in volta; - concordare appuntamenti successivi (per monitorare la situazione e raccogliere ulteriori dettagli utili);	- accogliere il presunto bullo in una stanza tranquilla, non accennare prima al motivo del colloquio; - iniziare il colloquio affermando che si è al corrente dello specifico episodio offensivo o di prevaricazione; - fornire al ragazzo/a l'opportunità di esprimersi, favorire la sua versione dei fatti; - mettere il presunto bullo di fronte alla gravità della situazione; - non entrare in discussioni; - cercare insieme possibili soluzioni ai comportamenti prevaricatori; - ottenere, quanto più possibile, che il presunto bullo dimostri comprensione del problema e bisogno di riparazione; - in caso di più bulli, i colloqui avvengono preferibilmente in modo individuale con ognuno di loro, uno di seguito all'altro, in modo che non vi sia la possibilità di incontrarsi e parlarsi; - una volta che tutti i bulli sono stati ascoltati, si procede al colloquio di gruppo;
	Colloquio di gruppo con i bulli
	- iniziare il confronto riportando quello che è emerso dai colloqui individuali; - l'obiettivo è far cessare le prevaricazioni individuando soluzioni positive;
Far incontrare prevaricatore e vittima – questa procedura può essere adottata solo se le parti sono pronte e il Team rileva un genuino senso di pentimento e di riparazione nei prepotenti; è importante: – ripercorrere l'accaduto lasciando la parola al bullo/i – ascoltare il vissuto della vittima circa la situazione attuale	

– condividere le soluzioni positive e predisporre un piano concreto di cambiamento
Coinvolgimento del gruppo classe o di possibili spettatori – Questa azione si consiglia solo quando possiamo rilevare un chiaro segnale di cambiamento nel presunto bullo (o più di uno) e il coinvolgimento del gruppo non implica esposizioni negative della vittima, ma può facilitare la ricostruzione di un clima e di relazioni positive nella classe.

cfr. Menesini E., Fiorentini G., Nocentini A., *Le azioni indicate per la gestione dei casi di bullismo e vittimizzazione nella scuola. I risultati della sperimentazione del progetto PEBUC (Protocollo di Emergenza per i casi di bullismo e cyberbullismo). Maltrattamento e abuso all'infanzia*.