



**Istituto Comprensivo Pescara 5**

Via Vincenzo Gioberti, 15 - 65123 Pescara

Dirigente Scolastico Prof.ssa Daniela Massarotto



**PEIC83400B**

# Documento di ePolicy

Misure atte a facilitare e promuovere l'utilizzo positivo  
delle TIC nella didattica e negli ambienti scolastici.

Misure di prevenzione e misure di gestione di situazioni problematiche  
relative all'uso delle tecnologie digitali.

Documento redatto in base alle indicazioni della piattaforma del MIUR

Generazioni Connesse



**Generazioni  
Connesse**  
SAFER INTERNET CENTRE



Co-financed by the European Union  
Connecting Europe Facility

# INDICE

## E-Safety Policy

### **1. Introduzione**

- 1.1. Scopo della Policy
- 1.2. Ruoli e Responsabilità
- 1.3. Condivisione e comunicazione della Policy all'intera comunità scolastica
- 1.4. Gestione delle infrazioni alla Policy
- 1.5. Monitoraggio dell'implementazione della Policy e suo aggiornamento
- 1.6. Integrazione della Policy con Regolamenti esistenti

### **2. Formazione e Curricolo**

- 2.1. Curricolo sulle competenze digitali per gli studenti
- 2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica e sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
- 2.3. Sensibilizzazione delle famiglie

### **3. Gestione dell'infrastruttura e della strumentazione ICT della scuola**

- 3.1. Accesso ad Internet: filtri, antivirus e sulla navigazione
- 3.2. Gestione accessi (password, backup, ecc.)
- 3.3. E-mail
- 3.4. Sito web della scuola e Registro elettronico
- 3.5. Social network
- 3.6. Protezione dei dati personali

### **4. Strumentazione personale**

- 4.1. Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc.
- 4.2. Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc.
- 4.3. Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc.

### **5. Rischi on line: conoscere, prevenire e rilevare**

- 5.1. Sensibilizzazione e Prevenzione
- 5.2. Cyberbullismo: che cos'è e come prevenirlo
- 5.3. Hate speech: che cos'è e come prevenirlo
- 5.4. Dipendenza da Internet e gioco online
- 5.5. Sexting
- 5.6. Adescamento online
- 5.7. Pedopornografia

## **6. Prevenzione, rilevazione e gestione dei casi**

- 6.1. Prevenzione
- 6.2. Rilevazione
- 6.3. Gestione dei casi
- 6.4. Cosa segnalare
- 6.5. Come segnalare
- 6.6. Gli attori del territorio
- 6.7. Allegati con le procedure

### **1. Introduzione**

L'Istituto Comprensivo Pescara 5 elabora il presente documento seguendo le indicazioni delle Linee di Orientamento per azioni di prevenzione e di contrasto al bullismo e cyberbullismo stabilite dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con "Generazioni Connesse" e il Safer Internet Center per l'Italia, recependo inoltre le integrazioni e le modifiche necessarie introdotte con la Legge 71/2017: "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo".

Questo documento è uno strumento flessibile e suscettibile di aggiornamenti successivi per rispondere alle richieste educative e pedagogiche derivanti dal costante e veloce cambiamento delle nuove tecnologie.

#### **1.1. Scopo della Policy**

La Policy ha lo scopo di educare e sensibilizzare tutti i componenti della comunità scolastica, gli alunni, gli insegnanti, i genitori, all'uso sicuro e consapevole di Internet.

I cosiddetti "nativi digitali" imparano a familiarizzare con le tecnologie fin dall'infanzia, ma, molto spesso, inconsapevoli dei rischi presenti nella rete. Gli insegnanti, che grazie all'uso delle TIC hanno l'opportunità di promuovere l'inclusione e l'eccellenza in ambito didattico attraverso la condivisione delle risorse, l'innovazione e la comunicazione, hanno anche la responsabilità di guidare gli studenti nelle attività online e di stabilire obiettivi chiari per un uso responsabile di Internet.

Il documento si pone pertanto come finalità, la promozione di un uso consapevole e critico delle tecnologie digitali e di Internet, l'acquisizione di procedure e competenze tecniche, nonché corrette norme comportamentali, senza trascurare la prevenzione, la rilevazione e la gestione di situazioni problematiche relative all'uso di tali tecnologie.

Dunque lo scopo della Policy è di precisare:

**1. misure atte a facilitare e promuovere** l'utilizzo delle TIC nella didattica, cioè azioni utili a sviluppare le competenze digitali;

**2. misure di prevenzione**, ossia azioni finalizzate alla prevenzione nella scuola di fenomeni legati ai rischi delle tecnologie digitali;

**3. misure per la segnalazione dei casi**, ovvero disposizioni semplici su come segnalare i casi nella scuola, comprese informazioni su chi sono le figure di riferimento, sugli strumenti a disposizione, sull'iter successivo alla segnalazione e su quali misure di tutela può contare chi segnala;

**4. misure per la gestione dei casi**, ossia le misure che la scuola attiva a supporto delle vittime, degli aggressori, delle famiglie e di tutti coloro che sono stati spettatori attivi o passivi di quanto avvenuto; misure che disciplinano anche il coinvolgimento di attori esterni quali le forze dell'ordine e i servizi sociali.

Questa Policy si applica a tutti i membri della comunità scolastica che hanno accesso o che sono utenti dei sistemi informatici della scuola.

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

## **1.2. Ruoli e responsabilità**

### **Dirigente Scolastico**

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

- garantire la sicurezza (tra cui la sicurezza on-line) dei membri della comunità scolastica;
- garantire che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, nonché un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della Comunicazione (TIC);
- garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;
- comprendere e seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.

### **Referente per la prevenzione e contrasto al bullismo e cyberbullismo e Animatore digitale**

Il ruolo del Referente per la prevenzione e contrasto al bullismo e cyberbullismo, in collaborazione con l'Animatore digitale, include i seguenti compiti:

- fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di Internet a scuola;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione).

## **Docenti**

Il ruolo del personale docente, fermo restando la libertà d'insegnamento, include i seguenti compiti:

- informarsi/aggiornarsi sulle problematiche inerenti la politica di sicurezza adottata dalla scuola nell'utilizzo delle tecnologie digitali e di Internet, rispettandone il regolamento;
- garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di Internet;
- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- promuovere incontri e laboratori dedicati alla Cittadinanza Digitale;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- far nascere nella componente studentesca una buona cognizione della proprietà del software e delle normative sul diritto d'autore, nonché far comprendere la necessità di effettuare ricerche sul web e la relativa estrazione di documenti evitando il plagio o l'illecita diffusione di dati personali;
- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta inadeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- non divulgare le credenziali di accesso agli account (username e password) e alla rete wifi;

- non allontanarsi dalla postazione lasciandola incustodita, se non prima di aver effettuato la disconnessione;
- non salvare sulla memoria locale delle postazioni, file contenenti dati personali e/o sensibili;
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo al Referente d'istituto per il bullismo e il cyberbullismo ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- segnalare al Dirigente Scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di Internet, nell'adozione delle procedure previste dalle norme.

## **Alunni**

Il ruolo degli alunni include i seguenti compiti:

- essere responsabili, in relazione al proprio grado di maturità e di apprendimento, nell'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- comprendere l'importanza di adottare buone pratiche di sicurezza on-line per non correre rischi, quando si utilizzano le tecnologie digitali;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- non eseguire tentativi di modifica della configurazione di sistema delle macchine;
- non utilizzare la strumentazione della scuola a scopi personali, ludici e/o ricreativi (a meno che l'attività didattica non lo preveda esplicitamente);
- non utilizzare propri dispositivi esterni personali senza aver acquisito il permesso da parte dell'insegnante;
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di Internet ai docenti e ai genitori.

## **Genitori**

Il ruolo dei genitori degli alunni include i seguenti compiti:

- sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;
- seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di Internet;

- concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di Internet;
- fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di Internet e del telefonino in generale.

### **1.3. Condivisione e comunicazione della Policy all'intera comunità scolastica**

L'Istituto si impegna a pubblicare sul sito della scuola il presente documento.

Inoltre, si prevede di:

1) Condividere e comunicare la politica di e-safety agli alunni:

- tutti gli alunni saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione;
- l'istruzione degli alunni riguardo all'uso responsabile e sicuro di Internet precede l'accesso alla rete;
- l'elenco delle regole per la sicurezza on-line sarà pubblicato in tutte le aule o laboratori con accesso a Internet;
- sarà data particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili.

2) Condividere e comunicare la politica di e-safety al personale:

- la linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di Internet sarà discussa negli organi collegiali (consigli di interclasse/intersezione, collegio docenti) e comunicata formalmente a tutto il personale, con il presente documento e altro materiale informativo anche sul sito web;
- un'adeguata informazione/formazione on-line del personale docente nell'uso sicuro e responsabile di Internet, sia professionalmente che personalmente, sarà fornita a tutto il personale, anche attraverso il sito web della scuola;
- tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

3) Condividere e comunicare la politica di e-safety ai genitori:

- l'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di Internet sarà attirata nelle news o in altre aree del sito web della scuola;
- sarà incoraggiato un approccio di collaborazione nel perseguire la sicurezza nell'uso delle TIC e di Internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali;

- il Referente per le attività di prevenzione e contrasto al bullismo e cyberbullismo fornirà ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di Internet anche a casa;
- i docenti di classe forniranno ai genitori indirizzi sul web, relativi a risorse utili per lo studio e a siti idonei ed educativi per gli alunni, sistemi di filtraggio e attività educative per il tempo libero.

#### **1.4. Gestione delle infrazioni alla Policy**

Per la componente alunni, le infrazioni verranno sanzionate, come da Regolamento di Istituto pubblicato sul sito web della scuola. Il Dirigente Scolastico ha facoltà di revocare l'accessibilità temporanea o permanente ai laboratori informatici e/o all'utilizzo di strumenti tecnologici (pc, tablet, notebook, ecc) a chi non si attiene alle regole stabilite.

In genere, sono previsti da parte dei docenti provvedimenti “disciplinari” proporzionati all'età e alla gravità del comportamento, quali:

- il richiamo verbale;
- il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);
- il richiamo scritto con annotazione sul diario;
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente Scolastico.

I genitori sono invitati a supportare la scuola per mettere a punto azioni di contrasto efficaci. Nel caso di infrazioni alla Policy si prevedono interventi, che vanno dalla semplice comunicazione del problema, alla convocazione e colloquio con il docente o il Dirigente Scolastico.

Per la componente docenti, le infrazioni alla Policy saranno gestite direttamente dal Dirigente Scolastico.

Qualora le infrazioni alla Policy si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. Si ricorda, infatti, che nel momento in cui un qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia (ex art. 331 del codice di procedura penale). L'omissione di denuncia costituisce reato (art. 361).

I reati che, in ambiente scolastico, possono essere riferiti all'ambito digitale e commessi per via telematica sono tra gli altri:

- minaccia, in particolare, se la minaccia è grave: per tale reato si procede d'ufficio (art. 612 codice penale);
- induzione alla prostituzione minorile (art. 600 bis);
- pedopornografia (art. 600ter);
- corruzione di minorenni (art. 609 quinquies).



- Per i reati sessuali la magistratura di norma procede su querela di parte; tuttavia nei casi più gravi si persegue d'ufficio e in genere i reati verso le/i minori sono tra quelli per i quali si procede d'ufficio.

## 1.5. Monitoraggio dell'implementazione della Policy e suo aggiornamento

Il monitoraggio dell'implementazione della Policy sarà compito del Referente per le attività di prevenzione e contrasto del bullismo e cyberbullismo. Si avranno inoltre degli aggiornamenti, laddove necessario e secondo una logica di condivisione e partecipazione attiva, sentito il parere degli insegnanti e viste le esigenze delle famiglie.

## 1.6. Integrazione della Policy con Regolamenti esistenti

La presente Policy si integra pienamente con il Piano Triennale dell'Offerta Formativa, il Regolamento interno di Istituto e il Patto di Corresponsabilità. Inoltre il nostro Istituto ha ricevuto l'invito a candidarsi per diventare Scuola eTwinning: ottenere lo status di Scuola eTwinning significa aver compiuto un percorso di sviluppo caratterizzato da elementi concretamente valutabili.

Le scuole premiate formano una rete europea di scuole leader in eTwinning e sono riconosciute come leader nelle seguenti aree:

- pratica digitale
- pratica dell'eSafety
- approcci innovativi e creativi alla pedagogia
- promozione dello sviluppo professionale continuo dello staff
- promozione di pratiche di apprendimento collaborativo per lo staff e gli studenti.



## 2. Formazione e Curricolo

### 2.1. Curricolo sulle competenze digitali per gli studenti

L'Istituto persegue, relativamente al curricolo digitale, le recenti indicazioni del PNSD: *"Definire le competenze di cui i nostri studenti hanno bisogno è una sfida ben*

*più ampia e strutturata di quella che il sentire comune sintetizza nell'uso critico della Rete o nell'informatica. Dobbiamo affrontarla partendo da un'idea di competenze allineata al ventunesimo secolo: fatta di nuove alfabetizzazioni, ma anche e soprattutto di competenze trasversali e di attitudini da sviluppare. In particolare, occorre rafforzare le competenze relative alla comprensione e alla produzione di contenuti complessi e articolati anche all'interno dell'universo comunicativo digitale, nel quale a volte prevalgono granularità e frammentazione.*

*Proprio per questo è essenziale lavorare sull'alfabetizzazione informatica e digitale (information literacy e digital literacy), che mettono al centro il ruolo dell'informazione e dei dati nello sviluppo di una società interconnessa basata sulle conoscenze e l'informazione.*

*È in questo contesto che occorre guardare alle sfide rappresentate dal rapporto fra pubblico e privato, dal rapporto tra creatività digitale e artigianato, e tra imprenditorialità digitale, manifattura e lavoro. Ed è ancora in questo contesto che va collocata l'introduzione al pensiero logico e computazionale e la familiarizzazione con gli aspetti operativi delle tecnologie informatiche. In questo paradigma, gli studenti devono essere utenti consapevoli di ambienti e strumenti digitali, ma anche produttori, creatori, progettisti. E i docenti, dalla loro parte e in particolare per quanto riguarda le competenze digitali, dovranno essere messi nelle giuste condizioni per agire come facilitatori di percorsi didattici innovativi basati su contenuti più familiari per i loro studenti".*

Inoltre si fa riferimento alle Indicazioni Nazionali del 2012, che riportano la definizione delle competenze-chiave (Raccomandazione del Parlamento Europeo e del Consiglio del 18 dicembre 2006 - 2006/962/CE), in ambito digitale:

*"La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione per il lavoro, il tempo libero e la comunicazione. Essa implica abilità di base nelle tecnologie dell'informazione e della comunicazione (TIC): l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet".*

## **2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica e sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali**

Il comma 124 della Legge n. 107/2015 dispone:

*“Nell'ambito degli adempimenti connessi alla funzione docente, la formazione in servizio dei docenti di ruolo è obbligatoria, permanente e strutturale. Le attività di formazione sono definite dalle singole istituzioni scolastiche in coerenza con il piano triennale dell'offerta formativa e con i risultati emersi dai piani di miglioramento delle istituzioni scolastiche previsti dal regolamento di cui al decreto del Presidente della Repubblica 28 marzo 2013, n. 80, sulla base delle priorità nazionali indicate nel Piano nazionale di formazione, adottato ogni tre anni con decreto del Ministro*

*dell'istruzione, dell'università e della ricerca, sentite le organizzazioni sindacali rappresentative di categoria”.*

Il corpo docente ha partecipato a corsi di formazione nell'ambito di piani nazionali, oltre che ad iniziative organizzate dall'istituzione e possiede generalmente una buona base di competenze e, nel caso delle figure di sistema, anche di carattere specialistico. Il nostro Istituto Comprensivo partecipa alle diverse iniziative promosse dal Miur sulla sicurezza in rete:

- “Un nodo blu”, campagna per la Giornata Nazionale contro il Bullismo e il Cyberbullismo a scuola;
- il Safer Internet Day (SID), la giornata mondiale per la sicurezza in Rete istituita e promossa dalla Commissione Europea con lo scopo di promuovere un uso responsabile, rispettoso, critico e creativo delle tecnologie digitali, soprattutto tra i bambini e i giovani, per rendere Internet un luogo positivo e sicuro;
- “Programma il Futuro”: insegnare in maniera semplice ed efficace le basi scientifico-culturali dell'informatica (pensiero computazionale). L'iniziativa, in collaborazione con il CINI - Consorzio Interuniversitario Nazionale per l'Informatica - fornisce alle scuole una serie di strumenti semplici, efficaci e facilmente accessibili per formare gli studenti alle basi scientifico-culturali dell'informatica che, nel loro insieme, costituiscono il cosiddetto "pensiero computazionale", essenziale affinché le nuove generazioni siano in grado di affrontare la società del futuro non come consumatori passivi ed ignari di tecnologie e servizi, ma come soggetti consapevoli di tutti gli aspetti in gioco ed attivamente partecipi del loro sviluppo.

Il percorso complesso della formazione specifica dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica e sull'utilizzo consapevole e sicuro di Internet può prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi.

### **2.3. Sensibilizzazione delle famiglie**

Le famiglie saranno informate della Policy e di tutte le azioni che essa promuove e condivideranno questo documento all'inizio dell'anno scolastico, unitamente al Regolamento d'Istituto. Potranno anche consultare, sul sito istituzionale della scuola, materiale relativo all'utilizzo delle TIC, tra cui la piattaforma “Generazioni Connesse”.

La scuola avrà cura di sensibilizzare le famiglie attraverso documentazione informativa ed incontri ad un corretto uso delle nuove tecnologie da parte dei ragazzi a casa e a scuola, indicando anche alcune semplici azioni che possono rendere la navigazione sicura. In modo particolare per quanto concerne l'accesso alle

attrezzature disponibili in classe (LIM e computer portatile) e nei laboratori, informerà sui regolamenti e la normativa vigente. Inoltre promuoverà l'uso delle nuove tecnologie al fine di assicurare un valore aggiunto alla formazione.

### **3. Gestione dell'infrastruttura e della strumentazione ICT della scuola**

#### **3.1. Accesso ad Internet: filtri, antivirus e sulla navigazione**

Per garantire che Internet sia uno strumento finalizzato ai soli scopi formativi, verrà esercitato costantemente il monitoraggio e l'aggiornamento dei programmi antivirus e saranno implementati sistemi di filtraggio e di identificazione di contenuti non educativi accessibili online, certificazioni, blocco di pop-up.

I computer fissi presenti nelle aule e nei laboratori accedono ad Internet attraverso rete LAN. I portatili collocati nelle aule accedono tramite WIFI. Tutti i computer presenti nella scuola hanno installato un antivirus. I docenti possono accedere con i loro dispositivi personali alla rete WIFI. Gli studenti possono accedere ad Internet in occasione di attività didattiche che si svolgono nel laboratorio informatico.

#### **3.2. Gestione accessi (password, backup, ecc.)**

La maggior parte delle aule del nostro Istituto sono dotate di un computer collegato alla Lim; alcuni richiedono l'inserimento di una password. Ogni docente è tenuto ad un controllo della strumentazione in aula, poiché l'uso del dispositivo non è permesso agli alunni. I computer si collegano alla rete tramite WIFI protetta da password, nota al personale docente. L'utilizzo di USB o CD personali è concesso solo con il permesso dei docenti.

#### **3.3. E-mail**

L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. La posta elettronica è protetta da antivirus, e quella certificata anche dall'antispam.

Qualora si preveda per alcune classi la creazione di account anche per gli studenti, sarà attivo solo il servizio Drive, poiché l'uso sarà esclusivamente didattico.

#### **3.4. Sito web della scuola e Registro elettronico**

Il sito web della scuola è gestito dalla Segreteria e dall'Animatore digitale; i genitori ad inizio anno scolastico esprimono o meno il proprio consenso all'utilizzo di foto e notizie relative agli alunni per l'aggiornamento del sito e per altre finalità.

Sono previste, inoltre, piattaforme virtuali di condivisione di materiali come Google Drive, Edmodo e altre, previa comunicazione e informazione alla famiglia.

Ogni docente accede al registro elettronico attraverso una password personale che non può essere comunicata a terzi.

Ogni famiglia riceve le credenziali per l'accesso riservato al registro elettronico, nel quale il corpo docente è tenuto a registrare assenze, valutazioni, note, argomenti delle lezioni e compiti.

L'uso del registro elettronico è spiegato alle famiglie nel corso del primo Consiglio di Classe/Interclasse dell'anno scolastico; attraverso il registro è anche possibile la condivisione di materiali tra i docenti e con gli studenti.

### **3.5. Social network**

La scuola non utilizza social network per la didattica.

### **3.6. Protezione dei dati personali**

La scuola osserva il rispetto della privacy dei propri utenti e protegge i dati personali che gli stessi conferiscono all'istituto. I dati personali vengono richiesti solo in caso di effettiva necessità e sono trattati in conformità alla normativa vigente (Decreto legislativo 30 giugno 2003, n. 196, c.d. Codice della Privacy). L'utente è sempre informato sulle finalità della raccolta dei dati personali al momento della stessa e ne firma, ove necessario, il consenso al trattamento. I dati personali dell'utente non sono comunicati a terzi senza il consenso dello stesso, fatti salvi i casi previsti dalla legge. Se l'utente decide di fornire alla scuola i propri dati personali, la scuola può comunicarli all'interno dell'Istituto o a terzi, che prestano servizi alla scuola.

## **4. Strumentazione personale**

### **4.1. Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc.**

Per gli studenti c'è il divieto di utilizzare all'interno della scuola smartphone e smartwatch. Tali dispositivi devono essere depositati in classe all'ingresso e ritirati all'uscita. È consentito agli alunni in difficoltà, con DSA e BES, di utilizzare il proprio tablet o notebook con il controllo del docente.

### **4.2. Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc.**

Durante le ore delle lezioni non è consentito l'utilizzo del cellulare per usi personali, mentre ne è consentito l'uso come quello di altri dispositivi elettronici a scopo didattico ed integrativo di quelli scolastici disponibili.

L'accesso alla rete WIFI dell'Istituto è disponibile per i docenti e protetta da password.

### **4.3. Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc.**

Durante l'orario di servizio al restante personale scolastico non è consentito l'utilizzo del cellulare.

## **5 - Rischi on line: conoscere, prevenire e rilevare**

### **5.1 - Sensibilizzazione e Prevenzione**

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

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

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

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

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

### **5.2 - Cyberbullismo: che cos'è e come prevenirlo**

La legge 71/2017 “Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo”, nell'art. 1, comma 2, definisce il cyberbullismo: “qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo”.

La stessa legge e le relative Linee di orientamento per la prevenzione e il contrasto del cyberbullismo indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;

sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);

promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education; previsione di misure di sostegno e rieducazione dei minori coinvolti; Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;

Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.

Nomina del Referente per le iniziative di prevenzione e contrasto che:

Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo.

A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.

Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

### **5.3 - Hate speech: che cos'è e come prevenirlo**

Il fenomeno di “incitamento all'odio” o “discorso d'odio”, indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona

(identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine “hate speech” indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;

promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;

favorire una presa di parola consapevole e costruttiva da parte dei giovani.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

### **5.4 - Dipendenza da Internet e gioco online**

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale?

## **5.5 – Sexting**

Il “sexting” è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti medialti sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

## **5.6 - Adescamento online**

Il grooming (dall'inglese “groom” - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di teen dating (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies – l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

## **5.7 – Pedopornografia**

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, concrete o simulate o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

La legge n. 269 del 3 agosto 1998 “Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù”, introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella legge n. 38 del 6 febbraio 2006 “Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet”, segna



una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Secondo la Legge 172/2012 - Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito [www.generazioniconnesse.it](http://www.generazioniconnesse.it) alla sezione "Segnala contenuti illegali" (Hotline).

Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children.

## **6. Prevenzione, rilevazione e gestione dei casi**

### **6.1. Prevenzione**

Il primo passo che la nostra scuola intende intraprendere è quello del coinvolgimento della comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online. È opportuno che i docenti, nell'espletamento delle proprie funzioni di formatori ed educatori, sappiano cogliere ogni opportunità per riflettere insieme agli alunni su tali rischi. Fondamentale è monitorare costantemente le relazioni interne alla classe, onde individuare possibili situazioni di disagio e intervenire tempestivamente, anche mediante il ricorso alle figure di sistema specializzate, per sostenere il singolo nelle situazioni di difficoltà personale e indirizzare il gruppo verso l'instaurazione di un clima positivo, di reciproca accettazione e rispetto, nelle situazioni di difficoltà socio-relazionale.

Tale percorso interno potrà essere ulteriormente rinforzato dalla partecipazione a progetti e/o iniziative esterne coerenti con i temi sopra menzionati, cui la scuola porrà

particolare attenzione, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità.

Tra i principali rischi dell'uso delle TIC ricordiamo:

- possibile esposizione a contenuti violenti e non adatti alla loro età;
- videogiochi diseducativi;
- pubblicità ingannevoli;
- accesso ad informazioni scorrette;
- virus informatici in grado di infettare computer e cellulari;
- possibili contatti con adulti che vogliono conoscere e avvicinare bambini/e o ragazzi/e, e adescamento on-line (grooming );
- rischio di molestie o maltrattamenti da coetanei (cyberbullismo);
- scambio di materiale a sfondo sessuale (sexting);
- uso eccessivo di Internet/cellulare (dipendenza)

## **6.2. Rilevazione**

I contenuti “pericolosi” comunicati/ricevuti a/da altri, messi/scaricati in rete, ovvero le tracce che possono comprovare l'utilizzo incauto, scorretto o criminoso degli strumenti digitali utilizzabili anche a scuola dai minori (l'eventuale telefonino/smartphone personale e il pc collegato a Internet) possono essere i seguenti:

- contenuti afferenti alla privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);
- contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);
- contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

## **6.3. Segnalazione e gestione dei casi**

Verranno seguiti i protocolli e le indicazioni operative suggerite dalla piattaforma “Generazioni Connesse” per la gestione dei singoli casi.

Nei casi meno problematici o quando il problema è ancora in fase iniziale, il singolo team di classe e/o Consiglio di classe può gestire la situazione autonomamente, previa comunicazione al Dirigente Scolastico (e, per conoscenza, al Referente per le

attività di prevenzione e contrasto al bullismo e al cyberbullismo), coinvolgendo i genitori degli interessati e la classe in attività di riflessione sul tema.

Nei casi gravi il docente che rileva il problema condivide quanto emerso con i colleghi e il Dirigente Scolastico, assieme al quale si valuterà il da farsi, anche rivolgendosi, per una consulenza, al numero 1.96.96 messo a disposizione da Telefono Azzurro.

Nei casi di maggiore gravità si valuterà anche il coinvolgimento di attori esterni quali le Forze dell'Ordine e i Servizi Sociali.

Le azioni poste in essere dalla scuola saranno dirette non solo a supportare le vittime, le famiglie e tutti coloro che sono stati spettatori attivi o passivi di quanto avvenuto, ma anche a realizzare interventi educativi rispetto a quanti abbiano messo in atto comportamenti lesivi, ove si tratti di soggetti interni all'Istituto.

#### **6.4. - Cosa segnalare**

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.

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. Esse, 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;**
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

Inoltre, la scuola **individua le figure che costituiranno un team** preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi 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.**

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo

sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

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

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

- **Cyberbullismo:** è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/le studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online:** se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting:** nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via 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.

## 6.5. - Come segnalare:

quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale 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.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due 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.
- **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.

Per tutti i dettagli fate riferimento 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.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

## 6.6. - Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi ad altre figure, enti, istituzioni e servizi presenti sul territorio qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse “Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani” (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

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

- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.

- **Co.Re.Com.** (Comitato Regionale per le Comunicazioni): svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale:** supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni:** accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali:** forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico:** segnalano
  - all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

## 6.7. - Allegati con le procedure

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

## Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

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

Avvisa il referente per il cyberbullismo (e/o il referente indicato nell'ePolicy) e il Dirigente Scolastico che convoca il CDC.

A) Se c'è fattispecie di reato - seguite le procedure della scuola

B) Se non c'è fattispecie di reato

- Richiedi la consulenza dello psicologo/a scolastico

- Informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto), se possibile con la presenza dello psicologo/a, 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.

- Valuta come coinvolgere gli operatori scolastici su quanto sta accadendo.

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

- Cerca di capire il livello di diffusione dell'episodio nell'Istituto e parla della necessità di non diffondere ulteriormente online i materiali.

- Parla del cyberbullismo e delle sue conseguenze (non nominare gli alunni coinvolti). Suggestisci di chiedere aiuto per situazioni di questo tipo. Prevedi un momento laboratoriale in modo da facilitare l'elaborazione della situazione.

- a seconda della situazione trova il modo di supportare la vittima e di responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.

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).

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

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

Sonda il clima di classe, ascoltando i ragazzi e monitorando ciò che accade (ma senza fare indagini o interrogatori). Cerca di capire il livello di diffusione dell'episodio a livello di Istituto.

Condividi con il referente per il cyberbullismo (e/o il referente indicato nell'e-policy): valuta con lui/loro le possibili strategie di intervento.

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.

Parla in classe del cyberbullismo e delle sue conseguenze (non nominare gli alunni che sospetti coinvolti). Suggestisci di **chiedere aiuto** per situazioni di questo tipo. Proponi attività in classe sull'empatia e sul riconoscimento delle emozioni (proprie e altrui)

**Se emergono evidenze passa allo schema successivo**

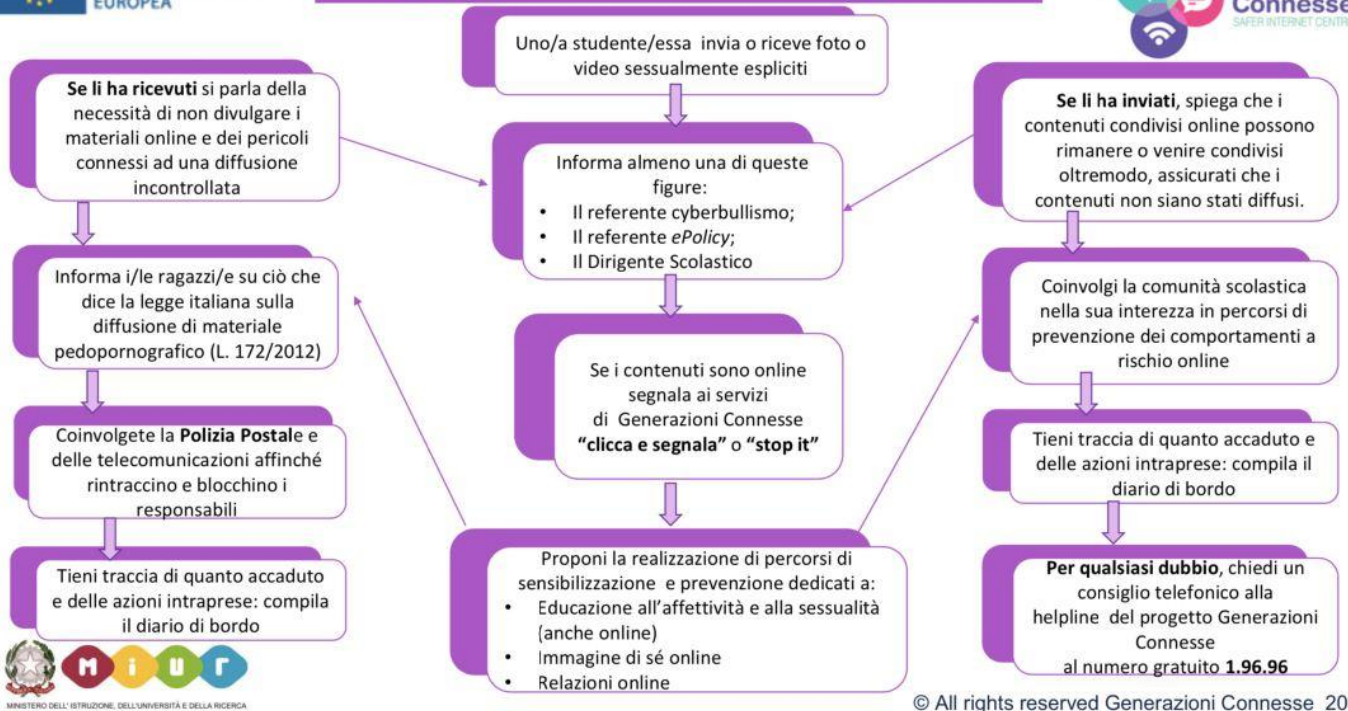
Valuta se è il caso di avvisare il consiglio di classe.  
Valuta se è il caso di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.

Informa i/le ragazzi/e su ciò che dice la legge italiana su cyberbullismo L. 71/2017)  
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

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

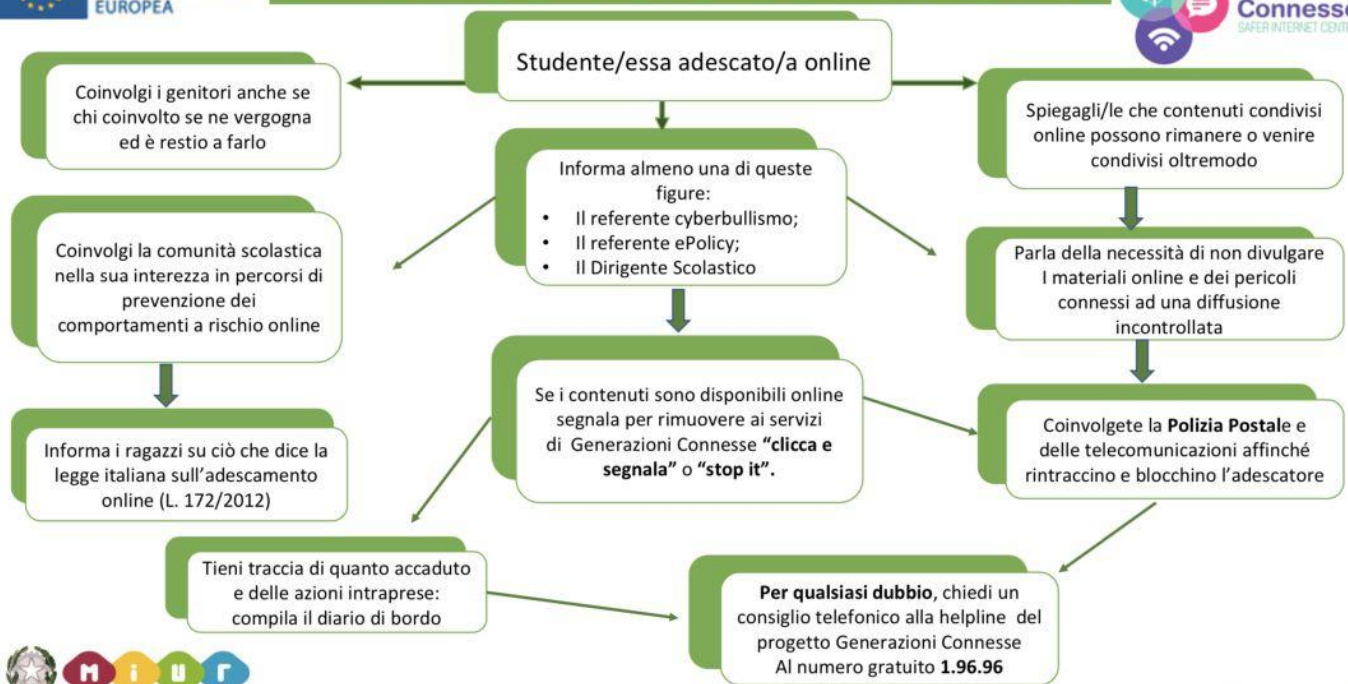


## Procedure interne: cosa fare in caso di Sexting?



## Procedure interne: cosa fare in caso di adescamento online?

## Procedure interne: cosa fare in caso di Adescamento Online?





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

