Ministero dell'Istruzione dell'Università e della Ricerca
Repubblica Italiana – Regione Siciliana

GELA IV CIRCOLO

CLEE014008@istruzione.it - VIA PALAZZI,148 GELA 93012 CL
Tel. 0933/930961 - Fax:0933832270
PEC: clee014008@pec.istruzione.it
www.capuanagela.it

E-Safety Policy

INDICE

Legge n. 71 del 29 maggio 2017

Introduzione

1. Scopo della Policy
- 1.1 Integrazione della Policy con Regolamenti esistenti.

2. Ruoli e Responsabilità
- 2.1 Dirigente Scolastico
- 2.2 Referente Cyberbullismo d'Istituto
- 2.3 Animatore Digitale e Team dell'Innovazione
- 2.4 Tecnico informatico
- 2.5 Direttore dei Servizi Generali e Amministrativi
- 2.6 Docenti
- 2.7 Personale ATA
- 2.8 Alunni
- 2.9 Genitori

3. Condivisione e Comunicazione della Policy all'intera comunità scolastica
- 3.1 Per il corpo docente
- 3.2 Per gli alunni
- 3.3 Per i genitori

4. Gestione delle Infrazioni della Policy
- 4.1 Infrazioni degli Studenti
- 4.2 Infrazioni del Personale Scolastico

5. Formazione e Curricolo
- 5.1 Curricolo Sulle Competenze Digitali per gli studenti
- 5.2 Formazione dei docenti sull'utilizzo consapevole e l'integrazione delle TIC nella didattica
- 5.3 Sensibilizzazione delle famiglie
- 5.4 Gestione dell'infrastruttura e della strumentazione ICT della scuola
- 5.5 Sito web della scuola
- 5.6 Social network

6. Strumentazione Personale
- 6.1 Per gli studenti: gestione degli strumenti personali - cellulari, tablet, ecc..
- 6.2 Utilizzo di personal device da parte degli studenti (BYOD):
- 6.3 Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc..
- 6.4 Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc..

7. Prevenzione, rilevazione e gestione dei casi
- 7.1 Prevenzione
- 7.2 Rilevazione

7.2.1 Che cosa segnalare
7.2.2 Come segnalare: quali strumenti e a chi
7.3 Azioni
7.3.1 Azioni di prevenzione
7.3.2 Azioni di primo intervento
7.4 Gestione dei casi
7.5 Segnalazione e denunce

8. Linee Guida
8.1 Linee guida per alunni
8.2 Linee guida per gli insegnanti
8.3 Consigli ai genitori per un uso responsabile di internet a casa

9. Allegati
- Allegato A: Materiale e link di collegamento, da inserire in una sezione dedicata sul sito web della scuola

Legge n. 71 del 29 maggio 2017

La legge 29 maggio 2017 n. 71 contenente " Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo si pone, così come statuisce l'art.1, "*l'obiettivo e la finalità di contrastare il fenomeno del cyberbullismo in tutte le sue manifestazioni, con azioni a carattere preventivo e con una strategia di attenzione, tutela ed educazione nei confronti dei minori coinvolti, sia nella posizione di vittime sia in quella di responsabili di illeciti, assicurando l'attuazione degli interventi senza distinzione di età nell'ambito delle istituzioni scolastiche."*

Per contrastare il fenomeno del cyberbullismo e del bullismo in generale occorre creare una rete di interventi in sinergia che richiede una stretta collaborazione tra la scuola (nella sua complessa organizzazione di agenzia formativa), le famiglie, le istituzioni, le forze dell'ordine e le associazioni del territorio.

Una efficace e incisiva attività di prevenzione del fenomeno del cyberbullismo richiede necessariamente la elaborazione dell'E-Safety Policy.

Introduzione

La Policy di e-safety è un documento autoprodotto dalla scuola, sulla base dell'indice ragionato messo a disposizione da Generazioni Connesse, sito del progetto Safer Internet Center per l'Italia, volto a descrivere una nuova visione del fenomeno della rete, le norme comportamentali e le procedure per l'utilizzo delle TIC in ambiente scolastico, le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse ad un uso non responsabile delle tecnologie digitali. La policy di e-safety dell'Istituto IV Circolo "Luigi Capuana" di Gela non è documento statico ma un lavoro destinato ad un maggiore approfondimento, per questo potrà essere revisionato annualmente da un gruppo di docenti formato sulle tematiche presenti nella policy.

1. Scopo della Policy

L'intento del nostro Istituto è quello di promuovere l'uso da parte degli alunni delle tecnologie digitali e di internet in modo responsabile, di far acquisire competenze e corrette norme comportamentali, di prevenire e gestire problematiche che derivano da un utilizzo pericoloso o dannoso delle tecnologie digitali.

I nostri allievi dimostrano un'innata predisposizione all'uso delle tecnologie, tuttavia, troppo spesso, a questa abilità si oppone una incapacità, dovuta alla giovane età, di non interpretare bene tutte le informazioni a cui, incessantemente, sono sottoposti, soprattutto attraverso l'uso dei social network. Pertanto la scuola attua parallelamente attività di prevenzione, controllo e formazione di docenti, allievi e famiglie. L'uso delle nuove tecnologie, se non adeguatamente usati, può trasformarsi in una trappola attraverso cui i giovani possono diventare vittime o carnefici di cyberbullismo.

Dunque, la policy di e-safety nasce dalla rilevazione di questo bisogno ed è volto a definire:

- le norme comportamentali e le procedure per l'utilizzo delle I.C.T.

nell'Istituto IV Circolo Didattico "Luigi Capuana", le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse a un uso non consapevole delle tecnologie digitali;

- prevenire fenomeni legati ai rischi delle tecnologie digitali;
- segnalare i casi individuati all'interno della scuola;
- gestire i casi, ovvero le misure che la scuola intende attivare a supporto delle famiglie e degli studenti vittime o spettatori attivi e/o passivi di quanto avvenuto.

Il Dirigente Scolastico, i docenti e l'Animatore Digitale hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di internet anche a casa, per prevenire il verificarsi di situazioni pericolose.

Per l'elaborazione del presente documento ci si è avvalsi del materiale bibliografico, reperibile in rete e messo a disposizione da Generazioni Connesse.

1.1 Integrazione della Policy con Regolamenti esistenti.

Il documento integra per obiettivi e contenuti i documenti che specificano le politiche dell'Istituto:

- PTOF, incluso il piano per l'attuazione del PNSD;
- Regolamento interno d'istituto;
- Regolamento per l'utilizzo dei laboratori di informatica.

L'Istituto, inoltre, opera in sinergia con le forze dell'ordine, con la Procura della Repubblica e con agenzie formative del territorio, al fine di mettere in campo strategie di prevenzione del cyberbullismo ed eventuali interventi di recupero (nel caso in cui vengano individuati episodi di tal genere), con il coinvolgimento di genitori/tutori dei minori interessati (sia in qualità di vittime che di autori), richiedendone espressamente la piena collaborazione.

2. Ruoli e Responsabilità

Nell'ambito di questa policy sono individuati i seguenti ruoli e le principali responsabilità correlate.

2.1 Dirigente Scolastico

Nel promuovere l'uso consentito delle tecnologie e di internet, il ruolo del Dirigente Scolastico è quello di:

- Garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- Garantire ai propri docenti una formazione di base sulle Tecnologie dell'Informazione e della Comunicazione (ICT) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse;
- Garantire l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on line;
- Dover informare tempestivamente, qualora venga a conoscenza di atti di cyberbullismo, che non si configurino come reato, i genitori dei minori

coinvolti (o chi ne esercita la responsabilità genitoriale o i tutori);
- Regolare il comportamento degli studenti ed imporre sanzioni disciplinari in caso di comportamento inadeguato, in relazione all'utilizzo delle TIC.

2.2 Referente Cyberbullismo d'Istituto

Il ruolo del Referente per Bullismo e Cyberbullismo include i seguenti compiti:

- Coordina iniziative di prevenzione e contrasto del cyberbullismo messe in atto dalla scuola, anche avvalendosi della collaborazione delle Forze di Polizia, nonché delle associazioni e dei centri di aggregazione giovanile presenti sul territorio;
- Costituisce l'interfaccia con le Forze di Polizia, con i servizi minorili dell'amministrazione della Giustizia, le associazioni ed i centri di aggregazione giovanile sul territorio, per il coordinamento delle iniziative di prevenzione e contrasto del cyberbullismo;
- Svolge un importante compito di supporto al Dirigente, nonché all'Istituzione scolastica, per la revisione/stesura di Regolamenti, atti e documenti (PTOF, PdM, RAV, modello di E-Safety Policy d'Istituto);
- Predispone documenti di rilevazione di incidenti di sicurezza in rete, attraverso la redazione di precisi format da protocollare;
- compila un prospetto per tenere traccia di eventuali segnalazioni (diario di bordo);
- Promuove la conoscenza e la consapevolezza riguardo a bullismo e cyberbullismo, attraverso progetti d'Istituto che coinvolgano genitori, studenti e personale scolastico;
- Facilita la formazione e la consulenza di tutto il personale;
- Raccoglie e diffonde buone pratiche educative, organizzative e azioni di monitoraggio, anche attraverso la periodica somministrazione di questionari;
- Collabora in team con altre figure scolastiche (Animatore Digitale e Team per l'Innovazione; Referente BES/Inclusione; Referente per la dispersione);
- segnala tempestivamente situazioni di rischio online o casi di bullismo o cyberbullismo;
- Supporta i Consigli di Interclasse e Intersezione ed i Coordinatori;
- Suggerisce, incentiva e supporta progetti di Istituto relativi allo sviluppo nei discenti delle Competenze di Cittadinanza e Costituzione, nonché progetti di prevenzione ed informazione/formazione dell'intera comunità scolastica;
- Coinvolge gli altri soggetti della comunità scolastica, con particolare attenzione agli studenti/ex studenti (PEER EDUCATION);
- Può attivare uno SPORTELLO anonimo di segnalazione.

2.3 Animatore Digitale e Team dell'Innovazione (come da PNSD):

Il ruolo dell'Animatore Digitale, coadiuvato dal "Team per l'Innovazione", include i seguenti compiti:

- Pubblicare il documento di E-Safety Policy sul sito della scuola;
- stimolare la formazione interna all'istituzione negli ambiti di sviluppo della

"scuola digitale" e fornire consulenza ed informazioni al personale in relazione ai rischi online ed alle misure di prevenzione e gestione degli stessi;

- Monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle TIC e di internet a scuola, nonché approntarsi all'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- Assicurare che gli utenti possano accedere alla rete della scuola solo tramite passwords applicate e regolarmente cambiate;
- Controlla e coordina, con l'ausilio di un opportuno registro, la prenotazione dei laboratori, consentendo in tal modo di tenere traccia di orari, laboratori e supporti utilizzati da ciascuno;
- Curare la manutenzione e lo sviluppo del sito web d'Istituto per scopi istituzionali consentiti (istruzione e formazione);
- Coinvolgere l'intera comunità scolastica (alunni, genitori ed altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".

2.4 Personale con funzione strumentale informatica

Il ruolo personale con funzione strumentale informatica si compone dei seguenti compiti:

- Può controllare ed accedere a tutti i files della intranet;
- è l'unico a poter installare nuovi software al fine di evitare violazioni dei copyright;
- Limita attraverso un proxy l'accesso ad alcuni siti;

La scuola per tale funzione può avvalersi anche di una ditta esterna per la fornitura di servizi informatici, in tal caso la stessa dovrà garantire:

- la disponibilità del servizio in una forma adeguata, anche a fronte di eventi eccezionali come di guasti o malfunzionamenti.
- la continuità del servizio a copertura delle esigenze operative della scuola;

In caso vi sia una ditta esterna che gestisce e mantiene l'infrastruttura informatica, con possibilità quindi di poter accedere ai dati personali della scuola, bisognerà regolamentare i reciproci ruoli quali Titolare (l'istituto) e Responsabile esterno del trattamento (la ditta esterna) con apposito contratto. In tale caso l'istituto avrà anche l'onere di fornire alla ditta esterna le istruzioni relative al trattamento dei dati che quest'ultima andrà a gestire nello svolgimento della sua attività. Ciò comporterà, quindi, che anche tutti i soggetti esterni agli istituti scolastici che gestiscono attività, per conto di questi ultimi, che comportano il trattamento di dati personali dovranno adeguarsi alla disciplina introdotta dal Regolamento Ue 2016/679 applicabile in tutti gli Stati membri a partire dal 25 maggio 2018, noto come GDPR (General Data Protection Regulation) relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali.

2.5 Direttore dei Servizi Generali e Amministrativi

Il ruolo del D.S.G.A. include i seguenti compiti:

- assicurare, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione necessari ad evitate un cattivo funzionamento della dotazione tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate.

2.6 Docenti

Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti:

- Provvedere personalmente alla propria formazione/aggiornamento sull'utilizzo del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in Internet e dell'immagine degli altri: lotta al cyberbullismo);
- Supportare gli alunni nell'utilizzo consapevole delle tecnologie informatiche utilizzate a scopi didattici ed informarli/formarli sul divieto di plagio e sul rispetto della normativa vigente in merito ai diritti d'autore;
- Segnalare al Dirigente scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazioni;
- Supportare ed indirizzare alunni coinvolti in problematiche legate alla rete.
- Mantenere tutte le comunicazioni digitali con alunni e genitori/tutori a livello professionale e realizzandole esclusivamente attraverso canali ufficiali scolastici.

2.7 Personale ATA

Il personale è tenuto ad assicurarsi di:

- Avere adeguata consapevolezza riguardo alle questioni di sicurezza informatica, alla politica d'Istituto e relative buone pratiche;
- Aver letto, compreso ed accettato il presente documento di E-Safety Policy;
- segnalare qualsiasi abuso, anche solo sospetto, al Dirigente Scolastico e/o all'Animatore Digitale per le opportune indagini/azioni/sanzioni;
- Mantenere tutte le comunicazioni digitali con alunni e genitori/tutori a livello professionale e realizzandole esclusivamente attraverso canali ufficiali scolastici.

2.8 Alunni

Non va sottovalutato il ruolo degli studenti come primi attori del percorso di acquisizione della capacità di positiva gestione delle proprie competenze digitali: in tale ottica si rende indispensabile coinvolgere anche i più giovani, non solo quali destinatari, ma anche interlocutori attivi e propositivi di tutte le azioni e gli interventi volti alla piena attuazione della Policy.

In particolare, il ruolo degli alunni include i seguenti compiti:

- essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;
- conoscere la politica della scuola sull'uso di dispositivi mobili e sull'uso delle immagini;
- comprendere l'importanza di adottare buone pratiche di sicurezza online quando si utilizzano le tecnologie digitali, acquisire consapevolezza delle situazioni di rischio legate alla rete, telefoni cellulari, fotocamere digitali;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.
- Essere consapevoli del significato e della gravità di atti di cyberbullismo, a tutela della propria e altrui incolumità, al fine di evitare di perpetrare violazioni o, nei casi più gravi, reati punibili da parte della Magistratura;
- Comprendere l'importanza della segnalazione di ogni abuso, uso improprio, o accesso a materiali inappropriati, e conoscere il protocollo per tali segnalazioni;

2.9 Genitori

Genitori e tutori svolgono un ruolo cruciale nel garantire che i minori comprendano la necessità di utilizzare in modo sicuro, consapevole ed appropriato dispositivi digitali e mobili. Per tale scopo è necessario che essi:

- Leggano, comprendano ed accettino il documento di E-Safety Policy;
- Contribuiscano, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- Incoraggino l'impiego delle ICT da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza;
- Sostengano l'Istituzione scolastica nel promuovere le buone pratiche di e-safety e, dunque, seguano le linee guida sull'uso appropriato di immagini digitali e video registrati in occasione di eventi scolastici, anche al di fuori delle aule;
- Consultino periodicamente le sezioni del sito web loro dedicate, con particolare riguardo ed attenzione alla consultazione del registro elettronico;
- Agiscano in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole

stabilite;

- Rispondano per gli episodi commessi dai figli minori a titolo di culpa in educando (articolo 2048 del Codice civile). Infatti, sono esonerati da responsabilità solo se dimostrano di non aver potuto impedire il fatto. Ma nei casi più gravi per i giudici l'inadeguatezza dell'educazione impartita ai figli emerge dagli stessi episodi di bullismo, che per le loro modalità esecutive dimostrano maturità ed educazione carenti.

3. Condivisione e Comunicazione della Policy all'intera comunità scolastica

Onde evitare che l'adozione del presente documento rappresenti un mero atto formale, l'Istituto si impegna ad intraprendere una serie di azioni ed iniziative per la messa in atto della Policy. Oltre alla condivisione con l'intera comunità scolastica attraverso la pubblicazione sul sito della scuola, si possono prevedere, ad esempio:

3.1 Per il corpo docente:

- discussione in ambito collegiale sui contenuti, sulle pratiche indicate e su come declinare nel curriculo le tematiche d'interesse della policy;
- confronto collegiale, a cadenza annuale, riguardo alla necessità di apportare eventuali modifiche e/o miglioramenti alla policy vigente;
- elaborazione di protocolli condivisi di intervento.

Il personale della scuola riceverà un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso materiali resi disponibili anche sul sito web della scuola.

3.2 Per gli alunni

- All'inizio dell'anno, in occasione dell'illustrazione del regolamento d'istituto agli alunni da parte dei docenti, verrà presentata la policy insieme ai regolamenti correlati;

3.3 Per i genitori:

- le famiglie saranno informate in merito alla linea di condotta adottata dalla scuola per un uso sicuro e responsabile delle tecnologie digitali e di internet attraverso la condivisione del presente documento e di materiali informativi specifici sul sito web della scuola;
- al fine di sensibilizzare le famiglie sui temi dell'uso delle TIC saranno organizzati dalla scuola incontri informativi di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o stigmatizzare;
- Lettura e comprensione del Regolamento d'Istituto e sottoscrizione del Patto di Corresponsabilità.

4. Gestione delle Infrazioni della Policy

4.1 Infrazioni degli Studenti

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola utilizzando le TIC ed internet, messi a loro disposizione a fini puramente didattici, sono prevedibilmente le seguenti:

- uso improprio della rete per esprimere giudizi, infastidire o impedire a qualcuno di esprimersi liberamente o partecipare al dialogo didattico-educativo;
- l'invio incauto o non autorizzato di immagini, foto o dati sensibili;
- la condivisione di immagini non appropriate, violente, intime o troppo spinte;
- la comunicazione incauta e non autorizzata con sconosciuti o soggetti comunque estranei all'azione didattico-educativa;
- il collegamento a siti web non indicati e, dunque, non autorizzati dai docenti durante attività laboratoriali di qualsiasi genere.

I provvedimenti disciplinari da adottare da parte dei consigli di classe/interclasse nei confronti di alunni che abbiano commesso una o più infrazione alla policy, secondo quanto sopra, (in proporzione sia all'età dello studente sia alla gravità dell'infrazione commessa) saranno i seguenti:

1. richiamo verbale;
2. sanzioni estemporanee commisurate alla gravità della violazione commessa:
    a. (assegnazione di attività aggiuntive da svolgere a casa su temi di Cittadinanza e Costituzione);
3. nota informativa ai genitori o tutori mediante registro elettronico;
4. convocazione dei genitori o tutori per un colloquio con gli insegnanti;
5. convocazione dei genitori o tutori per un colloquio con il Dirigente scolastico.

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi di eventuali disagi causati; di ridefinizione delle regole sociali di convivenza, attraverso la partecipazione consapevole ed attiva degli alunni delle classi coinvolte; di prevenzione e gestione positiva dei conflitti; di moderazione dell'eccessiva competitività, promozione dei rapporti amicali e di reti di solidarietà, di promozione della conoscenza e gestione delle emozioni.

4.2 Infrazioni del Personale Scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico ed in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet sono quelle potenzialmente atte a determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli studenti:

- Utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli

studenti, estraneo all'attività di insegnamento od al proprio profilo professionale, anche tramite l'installazione di software od il salvataggio di materiali non idonei;

- Utilizzo delle comunicazioni elettroniche con genitori e/o alunni non compatibile con il proprio ruolo professionale;
- Trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- Diffusione delle password assegnate e custodia incauta degli strumenti e degli accessi, di cui potrebbero approfittare terzi;
- Carente istruzione preventiva degli studenti sul corretto e responsabile utilizzo delle TIC e di internet;
- Mancata o non attenta vigilanza degli studenti, che potrebbe favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- Insufficiente azione di contrasto a terzi in situazioni critiche; di interventi correttivi o di sostegno a studenti;
- Mancata segnalazione al Dirigente, all'Animatore Digitale, ai genitori, in situazioni critiche.

Il Dirigente Scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle norme di sicurezza, compreso l'accesso ad internet e la posta elettronica inviata/pervenuta a scuola; procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone copia per eventuali successive investigazioni.

Tutto il personale è tenuto a collaborare con il Dirigente Scolastico ed a fornire ogni informazione utile alle valutazioni del caso ed all'avvio di procedimenti che possono avere carattere organizzativo-gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

Le infrazioni alla Policy possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e/o genitori a docenti e/o ATA. Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. Infatti è bene sottolineare il fatto che, nel momento stesso in cui 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 del codice penale);
- Induzione alla prostituzione minorile (art. 600bis);
- Pedopornografia (art. 600ter);

- Corruzione di minorenne (art. 609quinqies).

Per i reati sessuali la magistratura di norma procede su querela di parte; tuttavia, nei casi più gravi, si persegue d'ufficio ed in genere i reati verso minori sono tra questi ultimi.

5. Formazione e Curricolo

5.1 Curricolo sulle competenze digitali per gli studenti

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.

Le Indicazioni Nazionali del 2012, in raccordo con il programma europeo Competenze chiave per un mondo in trasformazione, prevedono che al termine del primo ciclo di istruzione lo studente possegga buone competenze digitali e sappia usare con consapevolezza le tecnologie della comunicazione.

A differenza dei loro genitori e dei loro docenti, i ragazzi e bambini di oggi appartengono ad una generazione molto differente; essi sono nati "nella tecnologia", sono i nativi digitali.

Essere nativi digitali non significa saper utilizzare in automatico la tecnologia: per questo il ruolo della scuola è (ancora) essenziale; la scuola ora più che mai ha il ruolo, molto arduo (anche considerando l'età media dei docenti), di saper insegnare l'uso e il corretto uso della tecnologia.

Su queste indicazioni l'Istituto attiverà un percorso con i seguenti obiettivi:

- promuovere un uso consapevole delle nuove tecnologie;
- sensibilizzare e attivare gli studenti sui rischi e i pericoli derivanti da un uso non corretto dei social network;
- favorire lo sviluppo di una cittadinanza attiva e responsabile;
- educare e sensibilizzare i minori ai rischi associati all'utilizzo di piattaforme di condivisione;
- conoscere e acquisire consapevolezza su natura, ruolo e opportunità delle TSI nel quotidiano;
- distinguere il reale dal virtuale, pur riconoscendone le correlazioni;
- sviluppare le abilità di base nelle TSI (uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni);
- acquisire consapevolezza su come le TSI possono coadiuvare la creatività e l'innovazione;
- riflettere sulle problematiche legate alla validità e all'affidabilità delle informazioni disponibili.

In virtù della valenza trasversale delle competenze digitali, la loro acquisizione verrà promossa attraverso percorsi didattici disciplinari e/o interdisciplinari inerenti diverse aree, coerentemente con gli obiettivi individuati nel curricolo di Istituto.

5.2 Formazione dei docenti sull'utilizzo consapevole e l'integrazione delle TIC nella didattica

Come previsto dal PNSD, al fine di promuovere la condivisione di buone pratiche per un uso consapevole e sicuro delle ICT, e di prevenire e contrastare "ogni forma di discriminazione e del bullismo, anche informatico" (Legge 107/2015, art. 1, c. 7, l), l'Istituto aderisce, al progetto "Generazioni Connesse" coordinato dal MIUR, in partenariato col Ministero dell'Interno-Polizia Postale e delle Comunicazioni e con altre importanti associazioni per la tutela dei diritti dei minori.

Su queste indicazioni l'Istituto attiverà un piano d'azione:

- analizzare il fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica;
- promuovere la partecipazione del corpo docente ai corsi di formazione sull'utilizzo e l'integrazione delle TIC nella didattica;
- monitorare le azioni svolte per mezzo di un questionario di autovalutazione;
- organizzare incontri con esperti;
- formazione istituzionale in contrasto al bullismo e al cyberbullismo attraverso gli snodi formativi del MIUR:
- interventi su classi individuate dalla scuola stessa;
- interventi che vedono la presenza dell'intera comunità educante, compresi i genitori,
- la formazione dei referenti di istituto;
- formazione specifica di Istituto, legata alle esigenze formative rilevate;
- partecipazione a progetti internazionali con la finalità di condividere materiale e tecniche di prevenzione e gestione di casi di bullismo per possibilità di costruire una conoscenza collaborativa con altri paesi attraverso la piattaforma e-twinning.

Inoltre, il percorso della formazione specifica dei docenti 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.

L'istituto predispone una bacheca online per la messa a disposizione e la condivisione di materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di internet, collegata alla homepage del sito dell'Istituto dove sarà possibile trovare materiali informativi sulla sicurezza in Internet per l'approfondimento personale, per le attività con gli studenti e gli incontri con i genitori, link a siti specializzati e contributi dal sito "Generazioni connesse".

5.3 Sensibilizzazione delle famiglie

L'Istituto, attraverso la relativa bacheca virtuale relativa a "Generazioni connesse" del sito scolastico dà ampia diffusione, del presente documento di Policy e-

safety per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e favorire un'attiva collaborazione tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi a un uso non consapevole e critico del digitale, inoltre s'impegna a condividere materiali dedicati agli alunni e alle famiglie come guide in formato pdf e video, che possono fornire spunti di approfondimento.

Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso delle nuove tecnologie all'interno dell'Istituto (tablet e smartphone) o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo.

Allo scopo di mantenere viva l'attenzione delle famiglie sull'uso consapevole delle TIC, della rete e delle numerose situazioni di rischio online, l'Istituto promuoverà opportunità di incontro e formazione per le famiglie sui temi oggetto della Policy, offerte dal territorio, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità e la diffusione materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati e dalle forze dell'ordine.

Inoltre, al fine di mettere in evidenza e valorizzare il contributo degli studenti, l'Istituto predispone una sezione della bacheca online dove sarà possibile pubblicare i progetti realizzati dagli studenti della scuola nella giornata mondiale della sicurezza in rete.

Infine, per implementare azioni mirate a promuovere il contrasto al bullismo e al cyberbullismo ed incoraggiare il cambiamento di atteggiamenti e comportamenti verso queste di violenze, l'Istituto consiglia di seguire la campagna europea contro il bullismo attraverso il sito http://www.e-abc.eu/it/bullismo/.

5.4 Gestione dell'infrastruttura e della strumentazione ICT della scuola.

Gestione accessi (password, backup, ecc.)

- Nei computer presenti nei laboratori sono previsti diversi profili di accesso con password relative:
  - amministratore;
  - docente;
  - classe;
  - guest.

5.5 Sito web della scuola

La scuola ha un sito web nel quale sono pubblicati tutti i documenti relativi la sicurezza in rete e la prevenzione di rischi legati ad un uso inconsapevole o sbagliato della stessa (Vedasi "Allegato A" in Allegati)

5.6 Social network

L'istituto, ritenendo i social network degli strumenti moderni flessibili e diretti, attraverso cui pubblicizzare le iniziative della scuola, informare i genitori ed avvicinare gli utenti alla scuola, riconosce e sostiene la pagina istituzionale Facebook, all'indirizzo https://www.facebook.com/Direzione-Didattica-Quarto-Circolo-Gela-Luigi-Capuana-771837912924873 per la pubblicazione di eventi o attività della

scuola.

La pagina Facebook è da considerarsi come supporto e completamento del sito web d'istituto. Tale pagina dovrà essere utilizzata unicamente in coerenza con le funzioni e gli obiettivi della scuola.

Le pubblicazioni sul sito della scuola o sui social network devono avvenire nel rispetto del D.Lgs. n. 196/03 e successive modifiche e integrazioni alla luce delle disposizioni del Reg. 2016/679/U.E..

6. Strumentazione Personale

6.1 Per gli studenti: gestione degli strumenti personali - cellulari, tablet, ecc..

Come espresso nel patto di corresponsabilità, i telefoni cellulari, non verranno utilizzati durante le lezioni scolastiche, pertanto si chiede alle famiglie di non lasciare tali dispositivi ad alunne e alunni; In caso di possesso all'ingresso in aula, dopo l'appello, la componente studentesca deposita telefoni e altri dispositivi dentro un armadietto appositamente collocato in classe, la cui chiave è in custodia al corpo docente che si alterna durante le lezioni.

Se uno studente viola questa policy, il telefonino o altro dispositivo sarà ritirato temporaneamente dall'insegnante in orario e riconsegnati allo studente al termine delle lezioni. L'insegnante avrà cura di annotare sul registro la mancanza rilevata. Al ripetersi dell'infrazione il telefonino o altro dispositivo verrà in tutti i casi confiscato e lo si terrà in un luogo sicuro in ufficio di segreteria. I dispositivi mobili saranno consegnati dal Dirigente Scolastico solo ai genitori/tutore con delega.

Nel caso in cui debbano comunicare con la famiglia durante l'orario scolastico, gli studenti possono usare gratuitamente la linea fissa della scuola rivolgendosi a un operatore; allo stesso modo le famiglie devono chiamare il centralino della scuola se hanno assoluta necessità di parlare con i propri figli ed in pochi minuti lo studente si metterà in contatto con casa. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.

Si riporta di seguito la tabella con le sanzioni in caso di inosservanza del regolamento d'istituto:

Mancanza	**Frequenza**	**Provvedimento**	**Organo competente**
L'alunno non ha il cellulare spento o silenzioso (riceve chiamata/notifica di messaggio)	1^ volta	Richiamo verbale (con annotazione sul registro di classe e comunicazione alla famiglia sul libretto/diario)	Docente
	2^ volta	Nota sul registro di classe (con comunica-zione alla famiglia su libretto/diario) e inter-vento del Dirigente scolastico	Docente DS
	Uso reiterato	Convocazione della famiglia In seguito: provvedimento disciplinare	Coordinatore di classe DS Consiglio di classe

L'alunno utilizza il dispositivo per chiamate e/o messaggistica o altri usi non consentiti (giochi, ascolto musica, ecc.)	1^ volta	Nota sul registro di classe (con comunicazione alla famiglia su libretto/diario). Eventuale intervento del Dirigente Scolastico	Docente DS
	Uso reiterato	Convocazione della famiglia In seguito: provvedimento disciplinare	Coordinatore di classe DS Consiglio di classe
L'alunno usa dispositivi elettronici durante una verifica scritta		Ritiro della verifica e valutazione gravemente insufficiente della stessa. Nota sul registro di classe e comunicazione alla famiglia su libretto/ diario	Docente Consiglio di Classe
L'alunno effettua riprese audio/foto/video senza informare preventivamente il docente		Nota sul registro di classe e comunicazione alla famiglia su libretto/diario	Docente
L'alunno diffonde in modo non autorizzato immagini/video/audio, anche se eventualmente acquisiti con il permesso del docente. L'acquisizione senza permesso costituisce aggravante.		Intervento del Dirigente Scolastico. Convocazione della famiglia. Eventuale provvedimento disciplinare, a seconda della gravità. Eventuale denuncia agli organi di polizia.	DS Consiglio di classe Consiglio di Istituto

6.2 Utilizzo di personal device da parte degli studenti (BYOD):

È previsto l'uso dei personal device degli studenti che, pertanto, dovrebbero utilizzare la rete scolastica e non quella personale.

Il piano Nazionale Scuola Digitale promuove, con l'azione #6, un'apertura al BYOD: "La scuola digitale, in collaborazione con le famiglie e gli enti locali, deve aprirsi al cosiddetto BYOD (Bring Your Own Device), ossia a politiche per cui l'utilizzo di dispositivi elettronici personali durante le attività didattiche sia possibile ed efficientemente integrato."

Il Regolamento d'istituto viene pertanto aggiornato onde prevedere il BYOD. Il docente che prevede l'utilizzo didattico di dispositivi digitali personali da parte degli alunni avrà l'accortezza di informare preventivamente le famiglie.

Ai sensi della Direttiva Ministeriale n. 30 del 15 marzo 2007, con la condivisione della presente Policy, "le famiglie si assumono l'impegno di rispondere direttamente dell'operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone" a seguito di violazioni della presente policy".

Informerà inoltre gli alunni che l'utilizzo non consentito/non corretto dei dispositivi suddetti negli ambienti scolastici può configurarsi come violazione della privacy. È quindi perseguibile per legge, oltre che sanzionabile secondo il regolamento scolastico.

Alunni con bisogni educativi speciali (BES) devono avere la possibilità di utilizzare in classe i propri dispositivi personali, pc e tablet compresi, come strumenti compensativi, anche con accesso a internet. Gli insegnanti di classe avranno cura di vigilare sul corretto utilizzo di tali dispositivi.

6.3 Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc..

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

Durante il restante orario di servizio è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente mentre è permesso l'uso di altri dispositivi elettronici personali per attività funzionali all'insegnamento, ad integrazione di quelli scolastici disponibili.

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

L'uso di dispositivi elettronici personali è permesso solo per attività funzionali al servizio.

7. Prevenzione, rilevazione e gestione dei casi

Gli operatori della scuola, in modo particolare gli insegnanti, sono promotori e garanti della costruzione dialogica di un percorso formativo partecipato, e nel loro ruolo diventano confidenti degli alunni e delle loro esperienze.

Proprio per questo, gli insegnanti sono spesso i primi a rilevare le problematiche e i rischi che bambini e gli adolescenti possono trovarsi ad affrontare ogni giorno. Si pensi ai numerosi casi di bullismo e di cyberbullismo di cui gli insegnanti vengono a conoscenza e che si trovano ad affrontare durante l'anno scolastico.

È compito degli insegnanti imparare a riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente.

Tra questi, un'attenzione specifica andrà prestata ai fenomeni di bullismo/ cyberbullismo (quest'ultimo una forma di prepotenza virtuale attuata attraverso l'uso di internet e delle tecnologie digitali), di sexting (pratica di inviare o postare messaggi di testo e immagini a sfondo sessuale, come foto di nudo o semi-nudo, via cellulare o tramite Internet (Levick & Moon 2010) e adescamento o grooming (una tecnica di manipolazione psicologica, che gli adulti potenziali abusanti utilizzano online, per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata) (Glossario di "Generazioni connesse").

Tuttavia in orario scolastico, alcuni studenti, eludono la sorveglianza del personale della scuola, usano il cellulare, non solo per comunicare con i propri genitori, ma anche per navigare su internet, andando su siti non adatti e inviando materiali riservati (foto, video e altro). Così facendo, gli studenti possono incorrere anche a scuola nei rischi sopra descritti.

Tutte le infrazioni alla presente Policy andranno tempestivamente segnalate al Dirigente Scolastico, che avrà cura di convocare le parti interessate onde valutare le possibili azioni da intraprendere.

7.1 Prevenzione

Le tecnologie digitali offrono da tempo la possibilità di ampliare la propria rete di amicizie in modo quasi smisurato.

Avere molti amici nella vita virtuale, o molti followers, è elemento di grande popolarità e di vanto con gli amici della vita reale.

Non a caso, quindi, gli adolescenti aggiungono tra le proprie cerchie, in particolare sui loro profili social, "amici di amici" senza valutare attentamente a chi stanno dando accesso alle proprie informazioni, alle proprie foto, spesso ai luoghi che frequentano. È evidente l'ingenuità e l'imprudenza con cui bambini e adolescenti si approcciano a questa modalità di relazione e amicizia "online".

Questo li espone a rischi notevoli: tra gli altri, quello di condividere con sconosciuti l'accesso al loro mondo online, e quindi alle informazioni che potrebbero essere utilizzate in modo inaspettato e non sempre positivo.

Aiutare i propri alunni a tutelarsi è un compito importante dell'insegnante che contribuisce in questo modo alla loro tutela nella vita virtuale, con ripercussioni non banali nella vita reale. Egli ha il compito di:

- Insegnare a scegliere con cura chi frequentare online;
- monitorare costantemente le relazioni interne alla classe, onde individuare possibili situazioni di disagio attraverso lo strumento del "diario di bordo" (schema riepilogativo delle situazioni gestite legate a rischi online) ed intervenire tempestivamente;
- ricorrere 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;
- Attuare percorsi scolastici di educazione all'affettività, educazione alla cittadinanza ed alla convivenza civile, educazione al rispetto, educazione all'uso consapevole della rete;
- Integrare il curricolo d'istituto con progetti e/o iniziative esterne coerenti con i temi sopra menzionati;
- selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità.

Gli alunni possono mostrare segni di tristezza o di ansia o di risentimento nei confronti di compagni o di altri e riferire spontaneamente o su richiesta l'accaduto ai docenti. I fatti riferiti possono essere accaduti anche al di fuori della scuola. Anche confrontandosi periodicamente con gli alunni sui rischi delle comunicazioni on-line, i minori possono riferire di fatti o eventi personali o altrui che "allertano" l'insegnante. Una "prova" di quanto riferito può essere presente nella memoria degli strumenti tecnologici utilizzati, può essere mostrata spontaneamente dall'alunno, può essere presentata da un reclamo dei genitori, può essere notata dall'insegnante che si accorge

dell'infrazione in corso. Mentre il docente è autorizzato a controllare le strumentazioni della scuola, per controllare l'uso del telefono cellulare di un alunno si rivolge al genitore.

7.2 Rilevazione

La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti.

7.2.1 Che cosa segnalare

Qualora si riscontri la pubblicazione di:

- dati sensibili o riservati (foto, immagini, video personali, informazioni private proprie o di amici; l'indirizzo di casa o il telefono, ecc.);
- contenuti che possano considerarsi in qualche modo lesivi dell'immagine altrui (commenti offensivi, minacce, osservazioni diffamatorie o discriminatorie, foto o video denigratori, videogiochi che contengano un'istigazione alla violenza, ecc.);
- contenuti riconducibili alla sfera sessuale: messaggi, immagini o video a sfondo sessuale, come foto di nudo o seminudo, ecc.

7.2.2 Come segnalare: quali strumenti e a chi

Il personale della scuola, anche con l'ausilio tecnico dell'Animatore Digitale, provvederà a conservare le eventuali tracce di una navigazione non consentita su internet o del passaggio di materiali inidonei sui pc della scuola nonché la data e l'ora.

Nel caso di messaggi, si cercherà di risalire al mittente attraverso i dati del suo profilo. L'insegnante dovrà copiare e stampare i messaggi per fornire le eventuali prove all'indagine sugli abusi commessi e raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico, alla famiglia ed, eventualmente, alla Polizia Postale.

Qualora siano coinvolti più alunni, in qualità di vittime o di responsabili della condotta scorretta, le famiglie degli alunni in questione saranno convocate e informate tempestivamente per un confronto.

In base alla gravità dei fatti si provvederà:

- ad una comunicazione scritta tramite diario alle famiglie;
- ad una nota disciplinare sul registro on-line;
- ad una convocazione formale dei genitori degli alunni, tramite segreteria;
- ad una convocazione delle famiglie da parte del Dirigente scolastico;
- per i reati più gravi la scuola si rivolgerà direttamente agli organi di polizia competenti.

7.3 Azioni

7.3.1 Azioni di prevenzione

- diffondere un'informazione capillare rivolta al personale scolastico, agli

studenti e alle famiglie, sui rischi che i minori possono correre sul web, condividendo materiali messi a disposizione sul sito del progetto "Generazioni connesse";

- È opportuno promuovere campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni.
- Portare a conoscenza degli alunni che per la legge italiana il cyberbullismo, la diffusione e il possesso di materiale pornografico è reato e che una foto o un video diffuso in rete potrebbero non essere tolti mai più.
- Sensibilizzare la popolazione studentesca sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione.
- Coinvolgere i genitori per attivare forme di controllo della navigazione e monitorare l'esperienza online dei propri figli.
- Tutelare la privacy e informare sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farli rispettare.
- Promuovere la consapevolezza e le conoscenze sul cyberbullismo, attraverso corsi di formazione, seminari, dibattiti.
- Segnalare agli alunni l'esistenza di una linea di ascolto19696 attiva tutto l'anno 24 ore su 24 di telefono azzurro che raccoglie richieste di ascolto e di aiuto. Al servizio HOTLINE si possono segnalare, in forma anonima, contenuti pedopornografici e altri contenuti dannosi diffusi dalla rete. Sono a disposizione due servizi ÒClicca e SegnalaÓ di Telefono Azzurro e ÒStop-ItÓ di Save the Cildren per chiedere la rimozione dei contenuti illeciti.

Le azioni utili a impedire un utilizzo incauto, scorretto o criminoso degli strumenti digitali materiali inviati, scaricati, ricevuti o condivisi su dispositivi digitali in uso a scuola (principalmente pc) sono:

- bloccare l'accesso a un sito o a un insieme di pagine impedendone la consultazione;
- controllare periodicamente i siti visitati dagli alunni;
- utilizzare un software in grado di intercettare le richieste di collegamento e di respingere quelle non conformi alle regole stabilite dall'amministratore;
- affidare a un gruppo di docenti scelto le regole di filtraggio.
- dotare i dispositivi della scuola di filtri che impediscano l'accesso a siti web non adatti ai minori (black list).
- far rispettare il divieto di utilizzo di dispositivi digitali propri, quali cellulare, agli studenti in orario scolastico. Le dovute eccezioni (uso del cellulare per comunicazioni alunno-famiglia in occasione di uscite didattiche) andranno espressamente regolamentate e dovranno comunque avvenire sotto la supervisione diretta di un docente responsabile;

7.3.2 Azioni di primo intervento

L'obiettivo che l'insegnante deve proporsi dopo avere riconosciuto il pericolo è agire di conseguenza, con azioni di contrasto efficaci e mirate, rispetto ai rischi sopra elencati. Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli studenti in orario scolastico, vi sono le seguenti:

Possibili rischi e possibili azioni di primo intervento	
RISCHI	**AZIONI**
- **Flaming:** è l'atto di inviare deliberatamente un messaggio ostile e provocatorio - **Harassment**: come il primo caso, ma i messaggi sono esclusivamente diretti alla vittima - **Denigration:** insultare mettendo in giro voci e pettegolezzi spesso inventati - **Exclusion:** far sentire solo qualcuno, isolandolo dal gruppo https://www.generazioniconnesse.it/site/it/cyberbullismo-scuole/	A seguito della segnalazione, il Dirigente Scolastico avrà cura di contattare il docente per un colloquio finalizzato a valutare la necessità di effettuare uno o più interventi di osservazione in classe e, successivamente, di pianificare adeguati interventi educativi e, ove necessario, di coinvolgere le famiglie per l'attivazione di un percorso comune e condiviso di sostegno al disagio. Se il comportamento rilevato viola solo le norme di buona convivenza civile e di opportunità, occorre convocare i soggetti interessati per informarli e discutere dell'accaduto e concordare forme costruttive ed educative di riparazione.
Adescamento online (grooming) https://www.generazioniconnesse.it/site/it/adescamento-scuole/	Sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione. Qualora si venga a conoscenza di casi simili, occorre valutarne la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.
Cyberstalking: persecuzione on line incessante https://www.generazioniconnesse.it/site/it/cyberbullismo-scuole/	Campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni. I casi possono essere molto variegati, andando dal semplice scherzo di cattivo gusto via sms/Whatsapp a vere e proprie minacce verbali e fisiche, che costituiscono reato. Occorre confrontarsi con il Dirigente Scolastico sulle azioni da intraprendere.

Sexting: invio di foto o video a sfondo sessuale https://www.generazioniconnesse.it/site/it/sexting-scuole/ https://www.generazioniconnesse.it/site/it/pedopornografia-scuole/	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione. Verso la componente studentesca: inserimento nel curricolo di temi legati all'affettività, alla sessualità e alle differenze di genere. In casi simili, se l'entità è lieve occorre in primo luogo parlarne con alunne e alunni e rispettivi genitori, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. Manca spesso la consapevolezza, tra ragazzi e adulti, che una foto o un video diffusi in rete divengono di pubblico dominio e la diffusione non è controllabile. In casi di rilevante gravità occorre infor-mare tempestivamente il Dirigente Scolastico.
Impersonation: furto di identità https://www.generazioniconnesse.it/site/_file/documenti/Schede/Docenti/SCHEDE%20SITO_IL%20FURTO%20D_IDENTITA.pdf **Tricky o Outing:** il cyberbullo pubblica on line a nome altrui informazioni imbarazzanti (furto identità) https://www.generazioniconnesse.it/site/it/privacy-scuole/	Informazione sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farle rispettare. Qualora il comportamento rappresenti un vero e proprio illecito, il Dirigente Scolastico deve esserne informato in quanto a seconda dell'illecito sono previste sanzioni amministrative o penali.

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.

L'elemento fondamentale per una buona riuscita dell'intervento educativo è infatti la corretta, compiuta e convinta ristrutturazione dell'ambiente sociale in cui tale fenomeno si verifica, e in particolare delle relazioni nel contesto della classe.

Gli atteggiamenti degli alunni, così come quelli dei loro genitori, possono giocare un molto significativo nel ridurre la dimensione del fenomeno.

Gli interventi mirati sul gruppo classe sono gestiti in collaborazione dal team dei docenti della classe e d'intesa con le famiglie, ad esempio:

- con percorsi di mediazione volta alla gestione positiva del conflitto;
- con gruppi di discussione (circle time), con rappresentazioni e attività di role-play sull'argomento del bullismo, con le strategie del problem solving.

Vengono intrapresi anche i percorsi individualizzati di sostegno alle vittime, volti a incrementarne l'autostima e l'assertività e a potenziare le risorse di interazione sociale, mentre i prevaricatori sono destinatari di interventi mirati a smuoverne le competenze empatiche e a favorire una loro condivisione delle norme morali.

Nei casi di maggiore gravità si valuterà anche il coinvolgimento di attori esterni quali le forze dell'ordine e i servizi sociali con cui siglare forme di collaborazione.

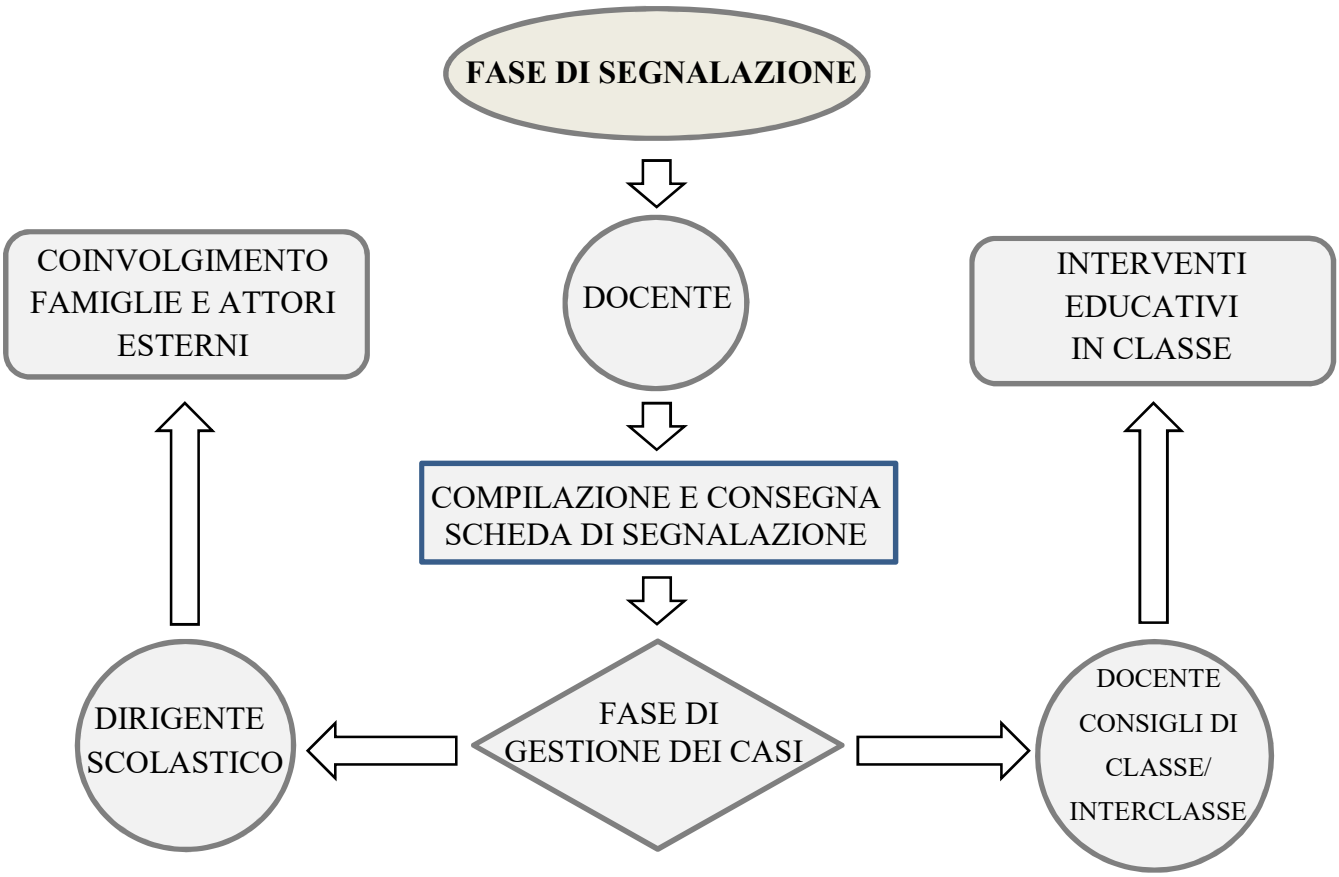
7.4 Gestione dei casi (Definizione delle azioni da intraprendere a seconda della specifica del caso)

La gestione dei casi rilevati va differenziata a seconda della loro gravità; è opportuno condividere ogni episodio con il team docenti.

Alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe, in altri è opportuno convocare genitori e alunni per cercare di rimediare all'accaduto. Nei casi più gravi occorre sottoporre all'attenzione del Dirigente Scolastico l'accaduto perché predisponga le azioni da intraprendere.

Per tutti i casi che costituiscono reato occorre informare il Dirigente Scolastico per confrontarsi sulle azioni da intraprendere ed eventualmente attivare l'intervento delle forze dell'ordine. Non esistono protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi, tuttavia si praticano forme di collaborazione nella prevenzione e contrasto del bullismo e del cyberbullismo con gli Enti Locali e le Forze dell'Ordine.

PROCEDURE OPERATIVE PER LA GESTIONE DEI CASI



7.5 Segnalazione e denunce

I docenti, in caso di sospetti o segnalazioni riguardo a episodi di cyberbullismo, creeranno situazioni adatte a favorire l'emersione delle vicende riferite, attraverso la presentazione alla classe di contenuti inerenti il problema, con relativa discussione di gruppo, o la stesura di elaborati scritti.

Laddove il docente colga possibili situazioni di disagio connesse ad uno o più di uno tra i rischi elencati nel paragrafo "*7. Prevenzione rilevazione e gestione dei casi*", dovrà informare il Dirigente Scolastico anche attraverso la compilazione di una "scheda di segnalazione" (di seguito allegata e disponibile nell'area riservata del sito web istituzionale). La scheda di segnalazione potrà essere redatta dal docente sia sulla base di eventi osservati direttamente a scuola, sia su eventi particolari che gli sono stati confidati dall'alunno o comunicati da terzi.

Esempio di SCHEDA DI SEGNALAZIONE

ALUNNO:		
CLASSE:		**SEZIONE:**
PROBLEMI EVIDENZIATI		
Osservazione diretta	Evento riferito	descrizione
		- **Flaming:** è l'atto di inviare deliberatamente un messaggio ostile e provocatorio - **Harassment**: come il primo caso, ma i messaggi sono esclusivamente diretti alla vittima - **Denigration:** insultare mettendo in giro voci e pettegolezzi spesso inventati - **Exclusion:** far sentire solo qualcuno, isolandolo dalgruppo
		Adescamento online (grooming)
		Cyberstalking: persecuzione on line incessante
		Sexting: invio di foto o video a sfondo sessuale
		Impersonation: furto di identità **Tricky o Outing:** il cyberbullo pubblica on line a nome altrui informazioni imbarazzanti (furto identità)
Firme		
Docenti coinvolti		

8. Linee Guida

8.1 LINEE GUIDA PER ALUNNI

- Non comunicare mai a nessuno la tua password e periodicamente cambiala, usando numeri, lettere caratteri speciali;
- Mantieni segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della tua scuola;
- Non inviare a nessuno fotografie tue o di tuoi amici;
- Prima di inviare o pubblicare su un BLOG la fotografia di qualcuno, chiedi sempre il permesso;
- Chiedi sempre al tuo insegnante a scuola o ai tuoi genitori a casa il permesso di scaricare documenti da Internet;
- Chiedi sempre il permesso prima di iscriverti a qualche concorso o prima di riferire l'indirizzo della tua scuola;
- Quando sei connessi alla rete RISPETTA SEMPRE GLI ALTRI, ciò che per te è un gioco può rivelarsi offensivo per qualcun altro;
- Non rispondere alle offese ed agli insulti;
- Blocca i Bulli: molti Blog e siti social network ti permettono di segnalare i cyber bulli;
- Conserva le comunicazioni offensive, ti potrebbero essere utili per dimostrare quanto ti è accaduto;
- Se ricevi materiale offensivo (e-mail, sms, mms, video, foto, messaggi vocali) non diffonderlo: potresti essere accusato di cyberbullismo;
- Rifletti prima di inviare: ricordati che tutto ciò che invii su internet diviene pubblico e rimane per SEMPRE;
- Riferisci al tuo insegnante o ai tuoi genitori se qualcuno ti invia immagini che ti infastidiscono e non rispondere; riferisci anche al tuo insegnante o ai tuoi genitori se ti capita di trovare immagini di questo tipo su Internet;
- Se qualcuno su Internet ti chiede un incontro di persona, riferiscilo al tuo insegnante o ai tuoi genitori;
- Ricordati che le persone che incontri nella Rete sono degli estranei e non sempre sono quello che dicono di essere;
- Non è consigliabile inviare mail personali, perciò rivolgiti sempre al tuo insegnante prima di inviare messaggi di classe o ai tuoi genitori prima di inviare messaggi da casa;
- Non scaricare (download) o copiare materiale da Internet senza il permesso del tuo insegnante o dei tuoi genitori;
- Non caricare (upload) materiale video o fotografico nei siti web dedicati senza il permesso del tuo insegnante o dei tuoi genitori.

8.2 LINEE GUIDA PER INSEGNANTI

- Evitate di lasciare le e-mail o file personali sui computer o sul server della scuola, lo spazio è limitato e di uso comune;
- Salvate sempre i vostri lavori (file) in cartelle personali e/o di classe e non sul desktop o nella cartella del programma in uso. Sarà cura di chi mantiene il corretto funzionamento delle macchine cancellare file di lavoro sparsi per la macchina e al di fuori delle cartelle personali;
- Discutete con gli alunni della policy e-safety della scuola, di utilizzo consentito della rete, e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di Internet;
- Date chiare indicazioni su come si utilizza Internet, ed eventualmente anche la posta elettronica, e informateli che le navigazioni saranno monitorate;
- Ricordate di chiudere la connessione (e di spegnere il computer) alla fine della sessione di lavoro su Internet e disabilitare la navigazione su Internet del laboratorio (qualora sia stata attivata);
- Ricordate agli alunni che la violazione consapevole della policy e-safety della scuola, di utilizzo consentito della rete, comporta sanzioni di diverso tipo;
- Adottate provvedimenti "disciplinari", proporzionati all'età e alla gravità del comportamento;
- Adottate interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi, di ridefinizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni;
- Nelle situazioni psico-socio-educative particolarmente problematiche, convocate i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi (sportello di ascolto psicologico gratuito, Servizi Sociali per la fruizione di servizi socio-educativi comunali, ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare);
- Chiedete/suggerite di cancellare il materiale offensivo, bloccare o ignorare particolari mittenti, uscire da gruppi non idonei, cambiare indirizzo e-mail, ecc…;
- Segnalate la presenza di materiale pedopornografico (senza scaricarlo o riprodurlo) alla Polizia Postale o al Telefono Azzurro o al Numero verde 800669696 (Ministero della Pubblica Istruzione: campagna "Smonta il bullo");
- In caso di abuso sessuale rilevato anche attraverso i nuovi mezzi di comunicazione come internet o il cellulare, confrontatevi con i colleghi di classe e il Dirigente Scolastico, denunciate all'autorità giudiziaria o agli organi di Polizia.

8.3 CONSIGLI AI GENITORI PER UN USO RESPONSABILE DI INTERNET A CASA

Consigli generali

- Posizionate il computer in salone o in una stanza accessibile a tutta la famiglia;
- Evitate di lasciare le e-mail o file personali sui computer di uso comune;
- Concordate con vostro figlio le regole: quando si può usare internet e per quanto tempo…
- Inserite nel computer i filtri di protezione: prevenite lo spam, i pop-up pubblicitari, l'accesso a siti pornografici;
- Aumentate il filtro del "parental controll" attraverso la sezione sicurezza in internet dal pannello di controllo;
- Attivate il firewall (protezione contro malware) e antivirus;
- Mostratevi coinvolti: chiedete a vostro figlio di mostrarvi come funziona internet e come viene usato per scaricare e caricare compiti, lezioni, materiali didattici e per comunicare con l'insegnante;
- Incoraggiate le attività on-line di alta qualità: ricercare informazioni scientifiche, ricercare nuovi amici nel mondo;
- Partecipa alle esperienze on-line: naviga insieme a tuo figlio, incontra amici on-line, discuti gli eventuali problemi che si presentano;
- Comunicate elettronicamente con vostro figlio: inviate, frequentemente, E-mail, Instant Message;
- Spiegate a vostro figlio che la password per accedere ad alcune piattaforme è strettamente personale e non deve essere mai fornita ai compagni o ad altre persone;
- Stabilite ciò che ritenete inaccettabile (razzismo, violenza, linguaggio volgare, pornografia);
- Discutete sul tema dello scaricare file e della possibilità di ricevere file con virus;
- Raccomandate di non scaricare file da siti sconosciuti;
- Incoraggiate vostro figlio a dirvi se vedono immagini particolari o se ricevono e-mail indesiderate;
- Discutete nei dettagli le conseguenze che potranno esserci se vostro figlio visita deliberatamente siti non adatti, ma non rimproveratelo se compie azioni involontarie;
- Spiegate a vostro figlio che le password, i codici pin, i numeri di carta di credito e i numeri di telefono e i dettagli degli indirizzi e-mail sono privati e non devono essere dati ad alcuno;
- Spiegate a vostro figlio che non tutti in Internet sono chi realmente dichiarano di essere; di conseguenza i vostri ragazzi non dovrebbero mai accordarsi per appuntamenti senza consultarvi prima;
- Il modo migliore per proteggere vostro figlio è usare Internet con loro, discutere e riconoscere insieme i rischi potenziali.

8.4 Consigli in base all'età

➢ Se tuo figlio ha meno di 8 anni

Seleziona con molta attenzione i siti "sicuri": ricordati che i gestori dei siti, per trarre il massimo guadagno, permettono agli inserzionisti di pubblicizzare i propri prodotti; Comunica a tuo figlio tre semplici regole:

 non dare il tuo vero nome, indirizzo e numero di telefono. Usa sempre il tuo "computer username" o nickname;

 se compare sullo schermo qualche messaggio o banner, chiudilo: insegna a tuo figlio come si fa;

 naviga esclusivamente sui siti autorizzati dai genitori: se vuoi andare su un nuovo sito, dobbiamo andarci INSIEME (molti siti richiedono la registrazione. Insegna a tuo figlio come registrarsi senza rivelare informazioni personali).

➢ Se tuo figlio ha tra gli 8 anni e i 10 anni

Progressivamente diminuisci la supervisione: dagli otto ai dieci anni permetti a tuo figlio di navigare da solo nei siti autorizzati, sottolineando che deve consultarti prima di esplorarne dei nuovi. Verifica periodicamente i contenuti dei siti "sicuri". Discuti con tuo figlio i rischi che possono presentarsi durante la navigazione on-line. Controlla, dalla cronologia il menu navigazione, se tuo figlio ha consultato siti non autorizzati per i quali non ti ha chiesto il permesso. Supervisiona l'e-mail di tuo figlio dopo averlo reso consapevole del fatto che hai pieno accesso alle sue comunicazioni.

Se tuo figlio vuole usare IM verifica che i suoi contatti siano limitati agli amici conosciuti. Specifica che non può inserire nuovi contatti senza averti prima consultato. Comunicagli che è assolutamente vietato cliccare su un link, contenuto in una E-mail, su un pop-up pubblicitario o su un banner (ricordati, infatti, che potrebbero presentarsi immagini pornografiche o che potrebbe avviarsi il download di "malware"). Incoraggia l'uso di internet per svolgere ricerche scolastiche. Definisci il tempo massimo di connessione ed incoraggia le attività con il mondo reale.

➢ Se tuo figlio ha tra gli 11 anni e i 13 anni

Tuo figlio è diventato grande e potrebbe dirti che il suo migliore amico ha la possibilità di navigare tutti i giorni a tutte le ore …. Che fare? Crea una partnership con i genitori dei migliori amici di tuo figlio in modo da concordare con loro le regole: tempi di connessione, fasce orarie, siti autorizzati, modalità di utilizzo di IM (messaggistica istantanea). Aiuta tuo figlio a creare una rete on-line sicura: siti controllati ed amici conosciuti.

9. ALLEGATI

Allegato A:

Materiale e link di collegamento, da inserire in una sezione dedicata sul sito web della scuola

1. Si allegano tre e-book interattivi per bambini, ragazzi e insegnanti, con consigli e giochi per navigare sicuri online:
   - GenerazioniConnesse-Kids.pdf
     https://www.generazioniconnesse.it/_file/documenti/KIt_Didattico/2015/GenerazioniConnesse-Kids.pdf
   - GenerazioniConnesse-Teens.pdf
     https://www.generazioniconnesse.it/_file/documenti/KIt_Didattico/2015/GenerazioniConnesse-Teens.pdf
   - GenerazioniConnesse-Docenti.pdf
     https://www.generazioniconnesse.it/_file/documenti/KIt_Didattico/2015/GenerazioniConnesse-Docenti.pdf

   In particolare, l'e-book dedicato ai docenti approfondisce alcune tematiche legate all'utilizzo di Internet e nuovi media offrendo spunti di riflessione e attività didattiche per condurre laboratori con bambini e ragazzi.

2. Eccoli tutti qui, con nome e cognome! I Super Errori sono le cattive abitudini, i click fatti con la testa tra le nuvole, le amicizie inopportune... In sostanza: i modi rischiosi di usare Internet! Conoscerli è il primo passo per evitarli. Anche perché basta un attimo di distrazione e... sono più vicini di quanto immagini!
   - **I Super Errori** https://www.generazioniconnesse.it/site/it/i-super-errori/
   - Chat Woman https://www.generazioniconnesse.it/site/it/ragazzi-chat-woman/
   - Silver Selfie https://www.generazioniconnesse.it/site/it/ragazzi-silver-selfie/
   - L'incredibile Url https://www.generazioniconnesse.it/site/it/ragazzi-incredibile-url/
   - L'uomo Taggo https://www.generazioniconnesse.it/site/it/ragazzi-uomo-taggo/
   - La ragazza Visibile https://www.generazioniconnesse.it/site/it/ragazzi-regazza-visibile/
   - Tempestata https://www.generazioniconnesse.it/site/it/ragazzi-tempestata/
   - Il Postatore Nero https://www.generazioniconnesse.it/site/it/ragazzi-postatore-nero/
   - **Le Armi segrete per sconfiggere i super errori**
     https://www.generazioniconnesse.it/site/it/le-armi-segrete/

   Sono tre, sono potentissime e puoi usarle in ogni momento per conquistare i Super poteri di Internet. Le armi segrete da sole non bastano, devi conoscere i Super Errori.

   - **L'inizio della Storia: Social network quando ti connetti, connetti anche la testa!**
     https://www.youtube.com/watch?v=BqtnYcfgLbM
   - **Quel bulletto del carciofo - 59 Zecchino d'Oro**
     https://www.serenacosta.it/genitori-e-figli/una-canzone-contro-il-bullismo-quel-bulletto-del-carciofo.html

- La canzone vuole rendere comprensibile ad un bambino il fenomeno del bullismo ma soprattutto vuole lasciare il messaggio che per contrastare il bullismo occorre unirsi e andare oltre i ruoli. Dietro ad un bullo ci può essere un bambino che usa la prepotenza solo perché è l'unico modo di entrare in relazione che conosce e, quindi, in realtà ha solo bisogno di affetto. La risposta al problema del bullismo proposta dal video è l'inclusione del bambino che si comporta da bullo piuttosto della continua esclusione.
  Per ascoltare la canzone "Quel bulletto del carciofo" è sufficiente cliccare sul link canzone vincitrice dello Zecchino d'Oro 2016.
  https://www.youtube.com/watch?v=tOSPsE_fzv4

- **Storie di ordinario cyberbullismo**

1) L'amore ingannevole

- L'amore ingannevole 1 (Io)
  https://www.youtube.com/watch?v=Wbr4Z2W9XtI&t=24s

  Io: quale scelta fare?
  - Soluzione 1 https://www.youtube.com/watch?v=2gQbnsp5HRs
  - Soluzione 2 https://www.youtube.com/watch?v=tHZIpv-VCb8
  - Soluzione 3 https://www.youtube.com/watch?v=JCWDCD3G_SY

- L'amore ingannevole 2 (l'Amica)
  https://www.youtube.com/watch?v=RDr_KdEe6RA

  L'amica: quale scelta fare?
  - Soluzione 1 https://www.youtube.com/watch?v=WJcaVudPzu8
  - Soluzione 2 https://www.youtube.com/watch?v=DIeKXf0Q004
  - Soluzione 3 https://www.youtube.com/watch?v=43zPQWt3XWI

2) Gaetano

- Gaetano 1
  https://www.youtube.com/watch?v=NwIb22Ydguk

  L'amica: quale scelta fare?
  - Soluzione 1 https://www.youtube.com/watch?v=XvD3SoF66lE
  - Soluzione 2 https://www.youtube.com/watch?v=KFjWcX3QgR4
  - Soluzione 3 https://www.youtube.com/watch?v=3mmgF1p7WHI

- Gaetano 2
  https://www.youtube.com/watch?v=wbJ7V6iKurE

  Gaetano: Quale scelta fare?
  - Soluzione 1 https://www.youtube.com/watch?v=UHxkAcgiA5o
  - Soluzione 2 https://www.youtube.com/watch?v=n1o0JUyNOCE
  - Soluzione 3 https://www.youtube.com/watch?v=xkHfHo5IFqo

Il Referente Scolastico

_____

Il Dirigente Scolastico

_____