**INTRODUZIONE** –

I/le ragazzi/e sono sempre più esposti, e sempre più precocemente, a occasioni di interazione con Internet attraverso una gamma via via più ricca di dispositivi facilmente alla loro portata. L'accesso a Internet, soprattutto per i bambini e adolescenti, rappresenta da una parte un'opportunità di accrescimento del sapere, di incremento delle capacità comunicative, di sviluppo delle competenze e di miglioramento delle prospettive di lavoro, ma dall'altra può esporre a situazioni di vulnerabilità che richiedono interventi specifici. In questi ultimi anni, è diventato sempre più forte il bisogno di adottare una strategia che si faccia carico di fornire risposte adeguate a "nuovi" bisogni. Questo implica lo sviluppo di servizi rivolti ai/alle ragazzi/e dal contenuto innovativo e di più alta qualità, che garantiscano loro di muoversi in sicurezza e con competenza negli ambienti digitali.

1. **Presentazione dell'ePolicy**
   - 1.1. Scopo dell'ePolicy
   - 1.2. Ruoli e responsabilità
   - 1.3. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
   - 1.4. Gestione delle infrazioni alla ePolicy
   - 1.5. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
   - 1.6. Integrazione dell'ePolicy 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 (Tecnologie dell'Informazione e della Comunicazione) nella didattica e sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
   - 2.3. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione** dell'infrastruttura **e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
   - **3.1. Accesso ad Internet**
   - **3.2. Gestione accessi**
   - **3.3. Strumenti personali**
   - **3.4. Strumenti di comunicazione online**
   - **3.5. Protezione dei dati personali**
4. **Rischi on line: conoscere, prevenire e rilevare**
   - **4.1. Sensibilizzazione e prevenzione**
   - **4.2. Cyberbullismo: che cos'è e come prevenirlo**
   - **4.3. Hate speech: che cos'è e come prevenirlo**
   - **4.4. Dipendenza da Internet e gioco online**
   - **4.5. Sexting e pedopornografia**
   - **4.6. Adescamento online**
5. **Prevenzione, segnalazione e gestione dei casi**
   - **5.1. Cosa segnalare**
   - **5.2. Come segnalare**
   - **5.3. Gestione dei casi**
   - **5.4. Monitoraggio**

1. Presentazione

L'ePolicy è un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie digitali positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo.
Nello specifico, è un documento programmatico autoprodotto dalla scuola volto a descrivere:

- il proprio approccio alle tematiche legate alle competenze digitali, alla sicurezza online e ad un uso positivo delle tecnologie digitali nella didattica;
- le norme comportamentali e le procedure per l'utilizzo delle Tecnologie dell'informazione e della comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione;
- le misure per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

1.1. Scopo della e-Policy

L'Istituto Comprensivo "Umberto I" di Pitigliano, consapevole del ruolo fondamentale della scuola nel dare risposte ai bisogni formativi della società e in piena sinergia con le sollecitazioni derivanti dalle politiche nazionali e comunitarie, si è impegnato a sostenere e realizzare obiettivi in tema di nuove tecnologie, linguaggi e comunicazione multimediale. Consapevole della valenza inclusiva del possesso delle competenze digitali, l'istituzione scolastica sta implementando ambienti tecnologici dedicati e, contestualmente, attivando percorsi di acquisizione di corrette norme comportamentali e di uso responsabile, sicuro, delle tecnologie digitali. In tale ottica ha avviato itinerari formativi sui temi della E-Safety, nell'ambito dei quali è stato elaborato il presente documento volto a definire norme comportamentali e procedure per l'utilizzo delle TIC nell'ambito dell'Istituto; misure atte a facilitare e promuovere l'utilizzo positivo delle TIC nella didattica e negli ambienti scolastici; misure per la prevenzione, per la rilevazione e la gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

1.2. Ruoli e responsabilità

Gli adulti hanno un ruolo fondamentale nel garantire che i minori siano in grado di utilizzare le tecnologie digitali in modo appropriato e sicuro. Quindi, sono coinvolti tutti coloro che svolgono una funzione educativa, oltre che formativa, primi fra tutti i genitori e la comunità scolastica nel suo complesso. Non va tuttavia sottovalutato il ruolo degli alunni come primi attori del percorso di acquisizione della capacità di positiva gestione delle proprie competenze digitali.

**-Il Dirigente Scolastico** è responsabile per la sicurezza dei dati, è informato sulle linee guida contenute nella e-Policy ed è garante della sua applicazione.
**- Il docente referente per la legalità e la prevenzione del bullismo e del cyberbullismo** opera in stretta collaborazione con il Dirigente scolastico, l'animatore digitale e il team digitale per promuovere comportamenti di consapevolezza e sicurezza online in tutta la comunità scolastica; facilita le procedure di gestione delle infrazioni tenendo un registro di incidenti di sicurezza
online; Cura la redazione e la revisione annuale del documento di e-Policy; coordina gli interventi di prevenzione e gestione di eventuali azioni di cyberbullismo.
**- L'animatore digitale** opera in stretta collaborazione con il D.S., con il docente referente per la legalità e la prevenzione del bullismo e del cyberbullismo e con i docenti del team digitale, curando la redazione e la revisione annuale del documento di e-Policy; favorisce la massima diffusione del documento; promuove azioni di formazione interna alla scuola negli ambiti del PNSD.
**- Il personale docente** promuove tematiche legate alla sicurezza online nella didattica e guida gli alunni nelle attività che prevedono l'accesso alla rete; segnala qualsiasi abuso, anche sospetto, al D.S. per le opportune indagini.

**-Direttore dei Servizi Generali e Amministrativi** assicura, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che le apparecchiature multimediali dei plessi scolastici siano funzionanti e sicure; garantisce il funzionamento dei diversi canali di comunicazione dell'istituzione scolastica (circolari, sito web, sportello ecc.) all'interno dell'istituzione scolastica, fra la scuola e le famiglie, per la notifica di documenti e la circolazione di informazioni del Dirigente Scolastico e dell'Animatore Digitale, anche sull'utilizzo delle tecnologie digitali e di internet.
**- Il personale ATA** è tenuto ad aver letto, compreso e sottoscritto la presente Policy, a collaborare con il personale docente segnalando qualsiasi abuso, anche sospetto, ai docenti responsabili, al Dirigente Scolastico o al docente referente per le opportune verifiche del caso.
**- I genitori** sostengono la scuola nel promuovere la sicurezza online, leggendo e sottoscrivendo la policy, partecipando agli incontri organizzati dalla scuola sui temi della sicurezza online e condividendo con la scuola le procedure previste in caso di violazione delle regole stabilite.
**- Le alunne e gli alunni** sono responsabili dell'utilizzo corretto delle tecnologie digitali e delle infrastrutture informatiche coerentemente con quanto previsto da questa policy. In particolare sono tenuti a:
- evitare l'utilizzo di dispositivi digitali personali durante le attività didattiche se non espressamente consentito dal personale docente, previa motivazione e finalità didattica;
- una corretta ricerca sul web, evitando il plagio, prestando attenzione a non diffondere dati personali propri e altrui;
- comprendere l'importanza della segnalazione di ogni abuso;
- essere consapevoli del significato e della gravità di atti di cyberbullismo;
- capire l'importanza di adottare buone pratiche di sicurezza informatica per evitare di commettere infrazioni e/o reati.
**-Gli Enti educativi esterni** le associazioni che entrano in relazione con la scuola devono conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC, promuovendo comportamenti sicuri.

**1.3**. Condivisione e comunicazione dell'e-Policy all'intera comunità scolastica.
Il presente documento è approvato dal Consiglio d'Istituto e sarà oggetto di condivisione di tutta la comunità scolastica. Verrà data ampia diffusione attraverso la pubblicazione all'albo della scuola, sul sito web istituzionale e la trasmissione via e-mail a tutto il personale dell'istituzione scolastica. Gli alunni saranno informati che l'uso di Internet e di ogni dispositivo digitale avverrà solo su autorizzazione e controllo degli insegnanti. La consapevolezza e la necessità di un uso sicuro e responsabile di internet saranno favorite da interventi e attività specifici sulla E-Safety. I genitori, durante gli incontri scuola-famiglia (collegiali e individuali), saranno incoraggiati ad instaurare un rapporto di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet.

**1.4 Gestione delle infrazioni alla Policy.**
Nel caso in cui un docente rilevi un'infrazione alle indicazioni della Policy è necessario che informi il coordinatore di classe, il quale a sua volta riferisce al Dirigente Scolastico e alla famiglia. Nel caso in cui l'infrazione si configuri come atto di cyberbullismo, il docente informa il referente per la legalità e la prevenzione del bullismo e del cyberbullismo. Nel caso si tratti di un reato è necessario che il Dirigente informi le autorità competenti (polizia postale).
Le potenziali infrazioni di alunne e alunni saranno seguite da interventi correttivi rapportati all'età e al livello di sviluppo del discente. I provvedimenti disciplinari avranno funzione educativa e saranno finalizzati a rafforzare la possibilità di recupero dello studente, a sviluppare il senso di responsabilità e a favorire il ripristino di rapporti corretti all'interno della comunità scolastica. In ogni momento sarà promossa l'azione educativa volta al rinforzo dei comportamenti corretti e rispettosi delle regole di policy.
Un primo intervento verrà attuato dal docente secondo le modalità indicate:
- richiamo verbale;
- richiamo verbale con annotazione disciplinare sul registro e sul diario personale;
- convocazione della famiglia.
Qualsiasi infrazione dovrà essere segnalata al docente referente del bullismo e cyberbullismo e al Dirigente Scolastico per prendere eventuali provvedimenti.

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

Il Dirigente Scolastico è responsabile dell'implementazione della Policy all'interno dell'Istituto. L'Animatore Digitale (insieme al Team dell'innovazione digitale), il Referente per la legalità e la prevenzione del bullismo e del cyberbullismo, in accordo con il Dirigente Scolastico, partecipano alla revisione e all'aggiornamento del documento. L'aggiornamento del documento viene sottoposto all'approvazione del Collegio dei Docenti.

**1.6 Integrazione della Policy con Regolamenti esistenti.**

La Policy è coerente con quanto stabilito dalla Legge (Statuto delle studentesse e degli studenti della scuola secondaria DPR 24 giugno 1998 n. 249 modificato dal DPR 21 novembre 2007 n. 235; Legge 29 maggio 2017 n. 71 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo"; Legge 31 dicembre 1996 n. 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali") dai Regolamenti vigenti e dal Patto di Corresponsabilità.

**2. Formazione e Curricolo**

**2.1 Curricolo sulle competenze digitali per gli studenti**

Tali competenze vengono promosse in maniera trasversale dai docenti, sulla base delle loro pratiche di insegnamento. Al termine della scuola primaria e al termine del primo ciclo di istruzione le competenze digitali vengono certificate sulla base dei seguenti profili:

- primaria: usa le tecnologie in contesti comunicativi concreti per ricercare dati e informazioni e per interagire con soggetti diversi.
- secondaria di primo grado: usa con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo.

**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 piano di formazione di Istituto prevede due principali ambiti di intervento: - una formazione organizzata dal Miur che si svolge secondo le modalità e i tempi previsti dal PNSD e che si realizza attraverso gli snodi formativi; - una formazione interna all'Istituto, con formatori esterni o interni nella modalità di tutoring/laboratorio. Questo tipo di intervento si basa sulle esigenze formative espresse dai docenti, rilevate ad inizio d'anno dall'animatore digitale e dal team del PNSD. In aggiunta, sarà data massima diffusione ai corsi organizzati dalla scuola.

**2.3 Sensibilizzazione delle famiglie**

Il nostro istituto organizza incontri aperti alle famiglie e agli studenti con enti/esperti esterni, per sensibilizzare docenti, alunne, alunni e genitori sui temi della sicurezza online.

Anche nei prossimi anni si continuerà ad utilizzare questo approccio per la sensibilizzazione delle famiglie, con incontri che offriranno occasione di confronto e discussione sui rischi rappresentati dall'uso di cellulari, smartphone e chat line senza un'adeguata formazione in merito ai rischi derivanti da un uso inappropriato di tali dispositivi.

La scuola darà inoltre ampia diffusione, tramite il referente del bullismo e cyberbullismo e il sito dell'istituto, del presente documento di Policy 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 inappropriato del digitale.

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

**3.1 Accesso ad Internet**.

L'accesso alla rete Internet al Personale Docente viene consentito con la modalità di connessione "wireless" (mediante gli access point). Le alunne e gli alunni possono accedere alla rete Internet esclusivamente con dispositivi dell'istituzione scolastica, in occasione di attività didattiche e/o formative svolte nei laboratori sotto la responsabilità e la sorveglianza di un insegnante.

La rete Internet non può essere utilizzata per scopi vietati dalla legislazione vigente e gli utenti sono

direttamente responsabili, civilmente e penalmente, a norma delle vigenti leggi, per ogni attività svolta.
È vietato scaricare e/o installare software sui PC e/o mobile device della scuola senza preventiva autorizzazione del referente per la Sicurezza Informatica.
Nella pratica didattica, il docente ha un ruolo fondamentale di responsabilità nel favorire l'uso corretto della rete, guidando gli studenti nelle attività online, stabilendo obiettivi chiari di ricerca, insegnando le strategie appropriate nella definizione e nella gestione delle risorse digitali su Web.

**3.2 Gestione accessi**

Ad oggi, nelle scuole primarie e secondarie di primo grado, i docenti e gli alunni accedono liberamente, ai computer, sia nell'aula informatica che nelle classi. Per il prossimo anno, si adotterà una politica di accesso ai computer suddetti, mediante la creazione di account per i docenti e/o per le singole classi, protetti da password personali.
I docenti accedono tramite un dispositivo personale per la compilazione del registro elettronico.
La connessione alla rete wi-fi, per i docenti, è accessibile dietro credenziali fornite dalla segreteria

**3.3 Strumentazione personale**

Per gli studenti della Scuola Primaria e della Scuola Secondaria di primo grado è vietato l'utilizzo di telefoni cellulari e/o di altri apparecchi elettronici senza autorizzazione durante le ore di attività didattica (intervalli inclusi). È consentito a tutti gli alunni, in casi specifici concordati con il docente (uscite didattiche, produzioni multimediali, ecc.) l'utilizzo di dispositivi elettronici personali per scopi didattici. Per i docenti, durante il loro orario di servizio, è consentito l'utilizzo di dispositivi elettronici personali solo ed esclusivamente per fini didattici.
Per il personale ATA della scuola è vietato l'utilizzo di dispositivi elettronici durante l'orario di servizio.

**3.4 Strumenti di comunicazione online**

Gli strumenti di comunicazione esterna troviamo in primis il sito web della scuola raggiungibile all'indirizzo http://www.comprensivopitigliano.it/, Il Dirigente e lo staff verificano i contenuti destinati alla pubblicazione, mentre fra gli strumenti di comunicazione interna troviamo il registro elettronico con tutte le sue funzionalità, la classica e-mail, gli strumenti di messaggistica istantanea che però hanno sempre più funzionalità tipiche anche dei social network, whatsapp o ulteriori applicativi e piattaforme di lavoro condiviso e collaborativo come Google Classroom che possono essere ampiamente utilizzati anche per facilitare e rendere più partecipata la didattica e la comunicazione a scuola.
In tutte le classi di ogni ordine e grado è diffuso l'utilizzo della piattaforma Google Classroom, avendo adottato le applicazioni fornite da G Suite for Education.

**3.5 Protezione dei dati personali**

In fase di iscrizione degli alunni alla scuola i genitori sottoscrivono un'informativa sul trattamento dei dati personali in ottemperanza all'art. 13 D.Lgs 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).
All'inizio di ogni anno scolastico i genitori rilasciano il consenso all'utilizzo di materiale fotografico e audiovisivo riservato ed elaborati degli alunni per esporli anche in sedi diverse da quelle dell'Istituto quali pubblicazioni in formato digitale e siti web.
In caso di attività di ampliamento dell'offerta formativa, organizzate in collaborazione con Enti esterni, viene richiesto preventivamente ai genitori il consenso informato alle riprese audio/ video e al loro eventuale utilizzo per scopi didattici, informativi e divulgativi anche tramite pubblicazione su siti web.
L'accesso ai dati riportati nel registro elettronico (ritardi, assenze, note e valutazioni) è riservato ai genitori della Scuola Secondaria di primo grado tramite l'invio di una password di accesso strettamente personale.

**4. Rischi online: conoscere, prevenire e rilevare**

**4.1 Sensibilizzazione e prevenzione**

Il rischio online si configura come la possibilità per il minore di:
• commettere azioni online che possano danneggiare sé stessi o altri;
• essere una vittima di queste azioni;
• osservare altri commettere queste azioni.
È importante riconoscere questi fenomeni ma è altrettanto importante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano.
Il nostro Istituto intende intervenire per la sensibilizzazione e prevenzione.

La sensibilizzazione avviene a partire dalle classi quarte della scuola primaria e sino all'intero ciclo della secondaria di primo grado, si punta a informare ma soprattutto ad educare alla consapevolezza e alla riflessione sulle seguenti tematiche: - Uso o abuso di internet - Dipendenza dallo smartphone Utilizzo della rete - Consapevolezza dei pericoli della rete.
Prevenzione: oltre a promuovere le competenze previste dal curriculo digitale un accento particolare viene dato: - alla conoscenza dell'importanza di tutelare la propria privacy e quella degli altri (dati sensibili, password, foto, video) e dell'implicazioni legali in caso di trasgressione; - alla conoscenza delle regole o norme etiche da tenere in mente quando si naviga in rete, quando si pubblica e/o si condivide un contenuto; - alla riflessione di come sia possibile dietro uno schermo protetti dall'anonimato infrangere con facilità tali norme, essere vittime o artefici di azioni lesive e offensive della propria e altrui persona.

**4.2 Cyberbullismo**

Il cyberbullismo (detto anche "bullismo elettronico") è un'azione aggressiva, denigratoria o intimidatoria anch'essa intenzionale e reiterata, che può essere messa in atto da un individuo o da un gruppo di persone, utilizzando mezzi elettronici (sms, chat, internet ecc.), nei confronti di una persona che non può difendersi facilmente.
La prevenzione consiste nell'attivare campagne di sensibilizzazione e informazione anche con l'ausilio di progetti. I casi possono essere molto variegati, variando dal semplice scherzo di cattivo gusto via sms/Whatsapp a vere e proprie minacce verbali e fisiche, che costituiscono reato. Occorre confrontarsi con gli organi competenti sulle azioni da intraprendere.

**4.3 Hate speech.**

Si tratta di un fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti…) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona. 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, etc.) ai danni di una persona o di un gruppo. L'obiettivo è 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.

**4.4 La dipendenza da Internet e gioco online.**

Può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito a insaputa di altri) rappresenta un vero e proprio illecito. È bene convocare la famiglia e avvisare gli organi competenti. Può manifestarsi anche attraverso le ore trascorse online a giocare, pertanto rappresenta una questione importante per la comunità scolastica che deve attenzionare il fenomeno e fornire gli strumenti agli studenti e alle studentesse affinché questi siano consapevoli dei rischi che comporta l'iperconnessione. La scuola può insegnare molto da questo punto di vista se integra la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online. Si potrebbe riflettere insieme su: come trascorri il tempo on line? Quando aggiunge valore alla tua vita e quando ti fa perdere tempo? Quale atteggiamento potrei cambiare quando sono online? Che ruolo ha e deve avere la tecnologia (internet o il gioco) nella mia vita?

**4.5 Sexting e pedopornografia**

Il sexting (abbreviazione di sex – sesso e texting – messaggiare, inviare messaggi) indica l'invio e/o la ricezione di contenuti (video o immagini) sessualmente espliciti che ritraggono se stessi o gli altri. 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. Chi è immerso dalla nascita nelle nuove tecnologie spesso non è consapevole che una foto o un video diffusi in rete potrebbero non essere tolti mai più né è consapevole di scambiare o diffondere materiale pedopornografico. È bene informare i genitori della possibilità di attivare forme di controllo parentale della navigazione.
In casi di rilevante gravità occorre informare tempestivamente gli organi competenti per gli adempimenti del caso.
-Violazione della privacy Informazione sull'esistenza di leggi in materia di tutela dei

dati personali e di organismi per farle rispettare. 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.
Qualora il comportamento rappresenti un vero e proprio illecito, gli organi competenti devono esserne informati.

### 4.6 Adescamento online o grooming

Il grooming (dall'inglese "groom" - curare, prendersi cura) rappresenta 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. Il grooming definisce il percorso attraverso il quale gradualmente l'adulto instaura una relazione - che deve connotarsi come sessualizzata – con il/la bambino/a o adolescente.

## 5. Prevenzione, rilevazione e gestione dei casi

La scuola si impegna ad attrezzare le aule con dispositivi elettronici sicuri e protetti.
I docenti si impegnano ad organizzare per gli alunni momenti di riflessione sui temi dell'utilizzo consapevole di internet e a formarsi su queste tematiche.
I genitori si impegnano a prendere visione della E-safety Policy e a seguire le azioni promosse dalla scuola per l'utilizzo consapevole della rete.
Gli alunni si impegnano a rispettare i regolamenti e a partecipare attivamente alle occasioni di confronto su queste tematiche organizzate dalla scuola.
Per i rischi connessi all'utilizzo delle nuove tecnologie (grooming, cyberbullismo, furto di identità, sexting), la scuola si affida anche a consulenti esterni per organizzare incontri informativi rivolti agli alunni, ai genitori ed al personale.

### 5.1 Cosa segnalare

Può capitare che un alunno manifesti un'insofferenza nei confronti di un compagno o, al contrario, che un alunno si senta escluso o emarginato dai coetanei. In alcuni casi sono gli alunni stessi a rivolgersi ai docenti in cerca di aiuto, anche quando i fatti siano accaduti fuori dall'ambiente e dall'orario scolastico. La diffusione capillare dei social network tra i bambini e ancor più tra gli adolescenti, li espone sempre più spesso al rischio di inviare o condividere senza alcuna protezione materiali personali o riservati. Discutendo in classe dei rischi del web e confrontandosi sulle esperienze personali o dei propri coetanei, emergono spesso fatti che "allarmano" l'insegnante. Tuttavia, mentre l'insegnante ha la possibilità, anzi il dovere, di intervenire sui dispositivi digitali in uso a scuola, non può intervenire direttamente sui telefoni cellulari dei bambini senza un'esplicita autorizzazione delle famiglie.
Si considerano da segnalare tutte quelle situazioni che si configurano come episodi di cyberbullismo (caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona o un piccolo gruppo tramite un utilizzo irresponsabile dei social network), ma anche usi inappropriati della rete (siti d'odio, contenuti non adatti all'età degli alunni, ecc.).
I docenti di classe informano il referente per la prevenzione di bullismo/cyberbullismo. Il referente informa il Dirigente Scolastico, il quale procede ad informare le famiglie. Tutte le segnalazioni riportate dai docenti vengono registrate su apposita scheda (diario di bordo).

### 5.2 Come segnalare: quali strumenti e a chi

Il personale della scuola, anche con l'ausilio del personale ATA, dovrà provvedere a conservare le eventuali tracce di una navigazione non consentita su internet o del passaggio di materiali inidonei sui pc della scuola; la data e l'ora consentiranno di condurre più approfondite indagini; nel caso di
messaggi, si cercherà di risalire al mittente attraverso i dati del suo profilo. Sia nel caso di chat che di messaggi di posta elettronica, l'insegnante dovrà copiare e stampare i messaggi per fornire le eventuali prove dell'indagine sugli abusi commessi. Tali prove saranno utili anche ad informare la famiglia dell'alunno vittima di abuso, il Dirigente scolastico e, ove si configurino reati, la Polizia Postale. In ogni caso, sarà opportuna una tempestiva informazione delle famiglie in merito all'accaduto, anche per consentire ulteriori indagini e, in assenza di prove oggettive, di raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico ed, eventualmente, alla Polizia Postale.

**5.3 Gestione dei casi- cosa segnalare**
Per un'efficace gestione dei casi, i docenti si attengono alle modalità illustrate nello schema messo a disposizione da Generazioni Connesse (allegato).
La gestione dei casi rilevati andrà differenziata a seconda della loro gravità, ferma restando l'opportunità della condivisione a livello di Consiglio di Classe di ogni episodio rilevato, anche minimo.
Nei casi più lievi la questione potrà essere affrontata e risolta con la discussione collettiva in classe.
Altri casi potranno essere affrontati convocando genitori e alunne/i coinvolti per riflettere insieme su quanto accaduto e come rimediare. Infine, nei casi più gravi e in ogni ipotesi di reato, occorrerà valutare tempestivamente con il Dirigente Scolastico i provvedimenti da adottare partendo dal Regolamento di Istituto.
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.
La segnalazione dell'episodio di bullismo o cyberbullismo da parte della vittima o di chi ne sia a conoscenza dei fatti, attraverso la compilazione della scheda di prima segnalazione appositamente predisposta e messa a disposizione della comunità scolastica, presa in carico da parte del team entro 2gg. Alla raccolta di informazioni da parte del team, Dirigente e/o referente e dei docenti coinvolti seguono la valutazione e la scelta dell'intervento. Il team del bullismo e cyberbullismo, il coordinatore della classe alla quale appartiene la vittima (o l'insegnante informato sui fatti) con la supervisione del referente o del Dirigente, decideranno l'intervento da attuare. Si prediligeranno interventi di tipo educativo e non punitivo, sanzioni disciplinari di tipo riparativo, convertibili quando possibile in attività a favore della comunità.
In seguito alla valutazione del singolo caso, attraverso la scheda di valutazione, al quale verrà attribuito un indice di gravità in base al livello di sofferenza della vittima, il team potrà individuare le azioni d'intervento più adatte.
**Codice verde**
-Incontro/i con gli studenti coinvolti
-Ripristino delle regole di convivenza all'interno della classe
-Interventi di educazione tra pari (peer education)
-Eventuale confronto con i genitori
-Confronto i con i docenti degli allievi

**Codice giallo**
-Interventi di sensibilizzazione: lezione dei docenti della scuola e incontri con esperti sui temi del bullismo e del cyberbullismo
-Counselling (sportello di ascolto psicologico)
-Interventi di educazione tra pari (peer education)
-Eventuale confronto con i genitori
-Confronto i con i docenti degli allievi

**Codice rosso**
**-** Provvedimenti disciplinari educativi (eventuale sospensione con obbligo di frequenza presso strutture convenzionate dove svolgere mansioni di pubblica utilità sociale).
-Eventuale segnalazione alle autorità (polizia postale, Garante per la protezione dei dati personali, Garante dell'Infanzia e dell'Adolescenza, servizi minorili dell'amministrazione della Giustizia, richiesta di ammonimento da parte del Questore).

**5.4 Monitoraggio e valutazione ex post**: osservazione e valutazione del comportamento di tutti gli alunni coinvolti con possibilità di interventi educativi di rinforzo.