Documento di ePolicy

BSIS036008

I.S.S. "TARTAGLIA-OLIVIERI"

VIA G. OBERDAN 12/E - 25128 - BRESCIA - BRESCIA (BS)

Laura Bonomini

Argomenti del Documento

Perché è importante dotarsi di una ePolicy

1. **Introduzione al documento di ePolicy**
    1. Scopo dell'ePolicy
    2. Ruoli e responsabilità
    3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
    4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
    5. Gestione delle infrazioni alla ePolicy
    6. Integrazione dell'ePolicy con regolamenti esistenti
    7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
2. **Formazione e curricolo**
    1. Curricolo sulle competenze digitali per gli studenti
    2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
    3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
    4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola:**
    1. Protezione dei dati personali
    2. Accesso ad Internet
    3. Strumenti di comunicazione online
    4. Strumentazione personale
4. **Rischi on line: conoscere, prevenire e rilevare**
    1. Sensibilizzazione e prevenzione
    2. Cyberbullismo: che cos'è e come prevenirlo
    3. Hate speech: che cos'è e come prevenirlo
    4. Dipendenza da Internet e gioco online
    5. Sexting
    6. Adescamento online
    7. Pedopornografia
5. **Segnalazione e gestione dei casi**
    1. Cosa segnalare
    2. Come segnalare: quali strumenti e a chi
    3. Gli attori sul territorio per intervenire
    4. Allegati con le procedure

Perché è importante dotarsi di una E-policy?

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

L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

Lo scopo della E-Safety Policy è di promuovere l'uso consapevole e critico delle tecnologie digitali e di Internet, seguendo le indicazioni di Educazione Civica Digitale emanate dal Miur, per salvaguardare e proteggere gli studenti e tutto il personale dell'Istituto; assistere il personale della scuola a lavorare in modo sicuro e responsabile; impostare chiare aspettative di comportamento e/o codici di condotta rilevanti per un uso responsabile di Internet a scopo didattico, personale o ricreativo; affrontare gli abusi online come il cyberbullismo; garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che il comportamento illecito o pericoloso è inaccettabile e che saranno intraprese le opportune azioni disciplinari e giudiziarie. Tenendo conto del piano d'azione elaborato, della sua complessità e della quantità delle azioni il documento potrà essere implementato e revisionato annualmente.

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse.

Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E- policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

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

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

La presente policy si applica a tutti i componenti della comunità scolastica che hanno accesso al sistema informatico della scuola o sono utenti dello stesso

---

1.2 Ruoli e responsabilità

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

DIRIGENTE SCOLASTICO

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

coinvolgimento attivo degli studenti anche attraverso modalità di peer education. Organizza e coordina il Team Antibullismo. Predispone eventuali piani di sorveglianza in funzione delle necessità della scuola. Tramite il sito web della scuola si forniscono le seguenti informazioni:

- nominativo/i del/i referente/i per il bullismo e cyberbullismo;
- contenuti informativi su azioni e attività di contrasto ai fenomeni di bullismo e cyberbullismo (Regolamento d'istituto, PTOF, Patto di corresponsabilità) oltre che di educazione digitale.

CONSIGLIO DI ISTITUTO

Approva il Regolamento d'istituto, che deve contenere possibili azioni sanzionatorie e/o riparative in caso di bullismo e cyberbullismo. Facilita la promozione del Patto di corresponsabilità tra scuola e famiglia.

COLLEGIO DOCENTI

All'interno del PTOF e del Patto di corresponsabilità predispone azioni e attività per la prevenzione dei fenomeni di bullismo e cyberbullismo, comprensive delle azioni di prevenzione primaria/universale specifiche per ogni ordine di scuola e delle azioni indicate rivolte a prendere in carico le situazioni di emergenza nella scuola. In modo particolare, organizza attività di formazione rivolte agli studenti sulle tematiche di bullismo, cyberbullismo ed educazione digitale. In relazione alle situazioni di emergenza, approva i protocolli di segnalazione e intervento promossi dal Team Antibullismo della scuola e collabora attivamente con il Team e le altre agenzie per la soluzione dei problemi.

Predispone gli obiettivi nell'area educativa, per prevenire e contrastare il bullismo e il cyberbullismo attraverso attività di curriculum scolastico. In tal senso, è importante legare la progettazione della scuola in un'ottica di Ministero dell'Istruzione prevenzione dei fenomeni di bullismo e cyberbullismo riferendosi a quanto previsto con la L. 92/2019 "Introduzione dell'insegnamento dell'Educazione civica", in particolare all'art. 3 "Sviluppo delle competenze e obiettivi di apprendimento" e all'art. 5 "Educazione alla cittadinanza digitale".

Partecipa alle attività di formazione per il contrasto dei fenomeni di bullismo e cyberbullismo organizzate da ogni autonomia scolastica, eventualmente avvalendosi di attività offerte da servizi istituzionali o enti qualificati presenti sul territorio (si vd. quanto proposto sulla piattaforma ELISA - www.piattaformaelisa.it)

PERSONALE DOCENTE

Tutti i docenti, venuti a conoscenza diretta o indiretta di eventuali episodi di bullismo o cyberbullismo, sono chiamati a segnalarli al referente scolastico o al Team Antibullismo d'istituto, al fine di avviare una strategia d'intervento concordata e tempestiva.

COORDINATORI DI CLASSE

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

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

COLLABORATORI SCOLASTICI E ASSISTENTI TECNICI

Svolgono un ruolo di vigilanza attiva nelle aree dove si svolgono gli intervalli, nelle mense, negli spogliatoi delle palestre, negli spazi esterni, al cambio dell'ora di lezione e durante i viaggi di

istruzione, ferme restando le responsabilità dei docenti.

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

Segnalano al dirigente scolastico e ai Team Antibullismo e per l'Emergenza eventuali episodi o comportamenti di bullismo e cyberbullismo di cui vengono a conoscenza direttamente e/o indirettamente.

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

L'ANIMATORE DIGITALE

L'Animatore digitale supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica); inoltre, monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola e ha il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

REFERENTE SCOLASTICO AREA BULLISMO E CYBERBULLISMO

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

TEAM ANTIBULLISMO

Coordina e organizza attività di prevenzione. Interviene nei casi acuti.Comunica al Referente regionale (anche tramite i Referenti territoriali), alla fine di ogni anno scolastico, i casi di bullismo o cyberbullismo.

I dati serviranno per un eventuale monitoraggio nazionale dei fenomeni di bullismo e cyberbullismo e potranno essere trasmessi dai Referenti regionali alla Commissione nazionale istituita presso il MI.

FAMIGLIE

Sono invitate a partecipare agli incontri di informazione e sensibilizzazione sui fenomeni di bullismo e cyberbullismo, favorendo una proficua alleanza educativa.

Firmano il patto di corresponsabilità educativa scuola-famiglia.

In questo contesto i genitori devono essere informati sul Regolamento d'istituto, sulle misure prese dalla scuola e sulle potenziali implicazioni penali e civili per il minore e per la famiglia come conseguenza di atti di bullismo e cyberbullismo. Sono chiamate a collaborare con la scuola nella prevenzione del bullismo e nelle azioni per fronteggiare le situazioni acute.

STUDENTI E STUDENTESSE

Partecipano alle attività di prevenzione del bullismo e del cyberbullismo organizzate dalla scuola.

Negli ordini di scuola dove sono previsti i rappresentanti degli studenti, in particolare nella scuola secondaria di secondo grado, i Rappresentanti di istituto e i due componenti eletti nella Consulta provinciale degli studenti collaborano con il Dirigente scolastico e il corpo docente all'organizzazione delle attività di prevenzione del bullismo e del cyberbullismo.

Sono chiamati a essere parte attiva nelle azioni di contrasto al bullismo e al cyberbullismo e di tutela

di chi ha subito, riferendo ai docenti e agli altri adulti gli episodi e i comportamenti di bullismo e cyberbullismo di cui vengono a conoscenza e supportando il/la compagno/a (consolandola e intervenendo attivamente in sua difesa).
Nella scuola secondaria di secondo grado sono chiamati a collaborare alla realizzazione di attività di peer education.
L'istituzione scolastica può favorire percorsi specifici in merito alla formazione dei rappresentanti degli studenti negli organi collegiali.
Enti educativi esterni e le associazioni che entrano in relazione con l'Istituto osservano le politiche interne sull'uso consapevole della Rete e della TIC.

1.3 Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.
Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.
Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).
Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto e di segnalare attraverso le modalità e gli strumenti che l'Istituto mette a disposizione, come indicato nel punto 1.5 del presente documento, atteggiamanti, atti e azioni, che destino sospetto e violino il codice di comportamento da parte degli studenti e delle studentesse.

1.4 Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/lle studenti/esse) si faccia a sua volta promotore del documento.

L'E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

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 prevedono delle attività di formazione:

per il corpo docente:

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

per la componente studentesca:

- discussione in classe con il coordinatore o personale formato sulla policy, nei primi giorni di attività scolastica, con particolare riguardo al protocollo di accoglienza per le nuove classi prime;
- diffusione tra gli studenti di un estratto del documento relativo, in particolare, ai comportamenti da attuare in caso di bisogno; lettura, comprensione e sottoscrizione del patto di corresponsabilità;

per i genitori:

- organizzazione di incontri 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.

1.5 Gestione delle infrazioni alla ePolicy

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni. E' bene che i docenti introducano, preventivamente, attività laboratoriali miranti a sviluppare nei loro alunni una sempre maggiore consapevolezza dei rischi legati a un uso imprudente e improprio del web e che forniscano loro, ogni qualvolta avvenga un'infrazione alle regole stabilite, gli strumenti per affrontare le

conseguenze dei loro errori. Ogni consiglio di classe definisce le attività inserendole nella programmazione annuale di educazione civica.

Infrazioni degli alunni a scuola o sulle piattaforme scolastiche

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;
- 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.
- utilizzo di un account non personale per accesso alla Gsuite di Istituto.

Gli esempi sopra sono stati indicati a titolo esemplificativo e non esaustivo. Qualora si presentassero altre casistiche che coinvolgano un uso improprio delle ICT sono anch'esse soggette all'e-policy.

I provvedimenti disciplinari da adottare da parte dei consigli di classe 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:

- richiamo verbale;
- il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante)
- sanzioni estemporanee commisurate alla gravità della violazione commessa (assegnazione di attività aggiuntive da svolgere a casa su temi di Cittadinanza e Costituzione);
- nota informativa ai genitori o tutori mediante registro elettronico;
- convocazione dei genitori o tutori per un colloquio con gli insegnanti;
- convocazione dei genitori o tutori per un colloquio con il Dirigente scolastico.
- sospensione dalle lezioni

Nel caso in cui l'infrazione si costituisca come reato, verrà effettuata segnalazione alle autorità competenti.

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.

Infrazione 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 ICT da parte degli alunni:

- 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 ICT e di internet;
- mancata o non attenta vigilanza degli studenti, che potrebbe favorire un utilizzo non autorizzato delle ICT 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 ICT 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.

Comportamenti a rischio in ambito famigliare

Compito precipuo dei genitori è supportare gli insegnanti e il personale scolastico nel riconoscimento e nella costruzione di azioni di contrasto efficaci ai principali rischi rappresentati dalla navigazione in internet di utenti molto giovani e spesso poco accorti. Nel caso di infrazione si prevedono interventi, rapportati alla sua gravità, che vanno dalla semplice comunicazione del problema alla convocazione da parte dell'insegnante di classe o del Dirigente Scolastico.

In considerazione dell'età degli alunni e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle ICT da parte degli alunni a scuola.

Le situazioni familiari meno favorevoli sono:

- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai;
- una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio;
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone;
- un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei;

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

1.6 Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E- policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E- policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

Il presente documento si integra pienamente con obiettivi e contenuti dei seguenti documenti, che specificano il contesto di attuazione delle politiche dell'Istituto per un uso efficace e consapevole del digitale nella didattica:

- PTOF, incluso il piano per l'attuazione del PNSD; Regolamento interno d'istituto.
- La policy richiede l'integrazione con l'inserimento delle seguenti norme:
- Utilizzo Del Laboratorio Di Informatica E Delle Postazioni Di Lavoro
- Autorizzazione per Gsuite Regolamento
- DDI

1.7 Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento

saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

Il monitoraggio dell'implementazione della Policy avverrà:

- alla fine di ogni anno scolastico, contestualmente al Rapporto di Autovalutazione e sulla base dei casi problematici riscontrati e della loro gestione;
- all'inizio di ogni anno scolastico, contestualmente alla revisione del PTOF, a cura del Dirigente scolastico, dell'Animatore digitale e dei collaboratori del Dirigente, a seguito di verifica atta a constatare l'insorgenza di nuove necessità e la revisione di tecnologie esistenti

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy. Organizzare
- incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di

regolamentare azioni e comportamenti.

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto per la stesura finale dell'ePolicy. Organizzare
- 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

Azioni da svolgere nei prossimi 3 anni:

- Organizzare uno o più eventi o attività volti a presentare il progetto e
- consultare i docenti dell'Istituto per la stesura finale dell'ePolicy. Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare
- azioni e comportamenti.
- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto per la stesura finale dell'ePolicy. Organizzare
- 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

Capitolo 2 - Formazione e curricolo

2.1 Curricolo sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali".

Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico" ("Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente", C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale.

Per quanto espresso l'Istituto si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale e con l'avvio di iniziative di sensibilizzazione alla cittadinanza digitale.

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 (rispettare i comportamenti nella rete e navigare in modo sicuro; prendere piena consapevolezza dell'identità digitale come valore individuale e collettivo da preservare);
- educare e sensibilizzare i minori ai rischi associati all'utilizzo di piattaforme di condivisione;
- conoscere e acquisire consapevolezza su natura, ruolo e opportunità delle ICT nel quotidiano;
- distinguere il reale dal virtuale, pur riconoscendone le correlazioni; sviluppare le abilità di base nelle ICT (uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni);
- acquisire consapevolezza su come le ICT 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 Educazione Civica dell' Istituto.

2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.
Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo
positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.
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 attiverà un piano d'azione:

- analizzare il fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle ICT nella didattica;
- promuovere la partecipazione del corpo docente ai corsi di formazione sull'utilizzo e l'integrazione delle ICT 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;
- la formazione dei referenti di istituto;
- formazione specifica di Istituto, legata alle esigenze formative rilevate;

2.3 Formazione dei docenti sull'utilizzo

consapevole e sicuro di Internet e delle tecnologie digitali

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.
La dirigenza promuove la partecipazione del personale ad iniziative istituite sia direttamente dalla scuola attraverso il piano annuale per la formazione dei docenti, sia dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dai docenti (anche online), purché coerenti con il piano di formazione.

2.4 Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.
L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.
L'Istituto, attraverso il sito scolastico darà 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 ICT, 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.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020)

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi)

Scegliere almeno 1 di queste azioni

- Effettuare un’analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un’analisi del fabbisogno formativo del corpo docente sull’utilizzo e l’integrazione delle TIC nella didattica.
- Effettuare un’analisi del fabbisogno formativo del corpo docente sull’utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare e promuovere per il corpo docente incontri formativi sull’utilizzo e l’integrazione delle TIC nella didattica.

Capitolo 3 - Gestione dell'infrastruttura e della strumentazione ICT della e nella scuola

3.1 Protezione dei dati personali

"Le scuole sono chiamate ogni giorno ad affrontare la sfida più difficile, quella di educare le nuove generazioni non solo alla conoscenza di nozioni basilari e alla trasmissione del sapere, ma soprattutto al rispetto dei valori fondanti di una società. Nell'era di Internet e in presenza di nuove forme di comunicazione questo compito diventa ancora più cruciale. È importante riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino". (cfr. http://www.garanteprivacy.it/scuola).

Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta, tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali. Il "corretto trattamento dei dati personali" a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni.

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8), tutelato dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

Anche le scuole, quindi, hanno oggi l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, entrato in vigore lo scorso 19 settembre.

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare riferimento all'uso delle tecnologie digitali, e indichiamo le misure che la scuola intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori. A tal fine, l'Istituto allega alla presente ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali. Il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Tutto il personale incaricato riceve poi istruzioni particolareggiate applicabili al trattamento di dati personali ai fini della protezione e sicurezza degli stessi. 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.

3.2 Accesso ad Internet

1. L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.
2. Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.
3. Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.
4. L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.
5. Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola". Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

L'accesso a internet è possibile nella nostra Istituto in tutte le aule, dotate di Lavagna Interattiva Multimediale o pannelli con relativo computer portatile e nei laboratori d'informatica. Le impostazioni sono definite e mantenute dal responsabile dei laboratori e dall'Animatore digitale ed è in carico a ciascun docente la segnalazione di malfunzionamenti e disservizi. I docenti hanno piena autonomia nel collegamento ai siti web nelle postazioni a loro riservate. Relativamente agli alunni che accedono a Internet durante l'attività didattica sono consentiti la navigazione guidata da parte dell'insegnante e la stesura di documenti collaborativi purché sotto il controllo dell'insegnante e nel caso in cui tale attività faccia parte di un progetto di lavoro precedentemente autorizzato.

La navigazione e l'accesso ad internet sono soggetti al filtro internet protetto della rete di Istituto.

3.3 Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

L'Istituto" Tartaglia-Olivieri "utilizza il registro elettronico "Classe Viva Spaggiari", sfruttandone al meglio tutte le potenzialità connesse, ciò permette di rendere immediate, trasparenti ed efficaci le comunicazioni all'interno della scuola e fra scuola e famiglie. Ogni famiglia riceve le credenziali, distintamente genitori ed alunni, per l'accesso riservato al registro elettronico, in cui il corpo docente è tenuto a registrare assenze, valutazioni, note e osservazioni.

I dati di contatto sul sito web sono: indirizzo della scuola, e-mail istituzionale e numero di telefono. Il sito prevede un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali, avvisi di carattere generale, e un'area riservata accessibile solo dopo autenticazione. Il Dirigente Scolastico si assume la responsabilità editoriale di garantire che il contenuto inserito dal personale autorizzato sia accurato e appropriato.

3.4 Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

La presente ePolicy contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Ministero dell'Istruzione per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

La presente ePolicy contiene indicazioni, di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Ministero dell'Istruzione per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device")

alvo casi del tutto eccezionali, gli smartphone e i telefoni cellulari non devono essere utilizzati a scuola; è permesso l'uso solo ai fini didattici con l'autorizzazione e lo stretto controllo dell'insegnante.

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. E' quindi perseguibile per legge, oltre che sanzionabile secondo il regolamento scolastico.
Se gli studenti utilizzeranno il dispositivo senza autorizzazione incorreranno nelle sanzioni previste del regolamento. Si ricorda che gli smartwatch sono equiparati all'uso dello smartphone.
Nel caso in cui debbano comunicare con la famiglia durante l'orario scolastico, alunne e alunni possono usare 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. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.

DOCENTI

Durante le ore delle lezioni, l'utilizzo dello smartphone così come di altri dispositivi elettronici personali è consentito solo a scopo didattico.

PERSONALE ATA

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

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022-2023).

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte deglistudenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti.
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.

Capitolo 4 - Rischi on line: 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 se stessi o altri;
- essere una vittima di queste azioni;
- osservare altri commettere queste azioni.

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

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

- Nel caso della sensibilizzazione si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.
- Nel caso della prevenzione si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.

Le principali aree di rischio possono essere riassunte come segue:

Contenuti

- l'esposizione a contenuti dannosi e non appropriati (es. contenuti razzisti ecc.);
- Siti web che promuovono stili di vita e comportamenti dannosi (es. siti che inneggiano al suicidio, che promuovono comportamenti alimentari scorretti, ecc.).

Contenuti che spingono all'odio.

- Validazione dei contenuti: come controllare l'autenticità e l'esattezza dei contenuti online.
- Pornografia.

Contatti

- Grooming (adescamento online), sfruttamento sessuale.
- Cyberbullismo e bullismo in tutte le forme.
- Il furto di identità, comprese le password.
- Pedopornografia (con questo termine si intende qualsiasi foto o video di natura sessuale che ritrae persone minorenni). CONDOTTE
- I comportamenti aggressivi (cyberbullismo e bullismo).

- Violazione della privacy, tra cui la divulgazione di informazioni personali o di dati (foto, video, voce) senza autorizzazione dei soggetti interessati.

Reputazione digitale

- Salute e benessere: dipendenza da Internet e quantità di tempo speso online, gioco d'azzardo o gambling, videogiochi online in comunità mondiali, l'immagine del corpo.
- Sexting.
- Copyright (poca cura o considerazione per la proprietà intellettuale e i diritti d'autore).

Al fine di minimizzare i rischi e gli effetti di attacchi informatici legati all'utilizzo di postazioni di lavoro in rete, (sia essa Intranet o Internet), la scuola è dotata dii firewall e delle misure minime di sicurezza come da nota MIUR 0003015 del 20-12-2017.

4.2 Cyberbullismo: che cos'è e come prevenirlo

La legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", nell'art. 1, comma 2, definisce il cyberbullismo:

"*qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo*".

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

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- nomina del Referente per le iniziative di prevenzione e contrasto che: Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio. Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Il cyberbullismo ("bullismo elettronico" o "bullismo in internet") è una forma di bullismo attuata attraverso l'uso dei Nuovi Media (dai cellulari a tutto ciò che si può connettere a internet). Come il bullismo tradizionale è una forma di prevaricazione e di oppressione reiterata nel tempo, perpetuata

da una persona o da un gruppo di persone più potenti nei confronti di un'altra persona percepita come più debole. Le caratteristiche tipiche del bullismo sono l'intenzionalità, la persistenza nel tempo, l'asimmetria di potere e la natura sociale del fenomeno (Olweus, 1996), ma nel cyberbullismo intervengono anche altri elementi, quali:

- l'impatto (viralità): la diffusione di materiale tramite internet è incontrollabile e non è possibile prevederne i limiti (anche se la situazione migliora, video e immagini potrebbero restare online).
- la possibile anonimità: chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile.
- l'assenza di confini spaziali: il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo dei suoi spazi-rifugio (è raggiungibile infatti anche a casa propria).
- l'assenza di limiti temporali: il cyberbullismo può avvenire a ogni ora del giorno e della notte.
- l'indebolimento dell'empatia: esistono cellule chiamate neuroni specchio che ci permettono di "leggere" gli altri quando li abbiamo di fronte, capirli e di provare emozioni simili a quelle che loro provano, proprio come se fossimo di fronte ad uno specchio. Quando le interazioni avvengono online la funzione speciale di questi neuroni viene meno.
- il feedback non tangibile: il cyberbullo non vede in modo diretto le reazioni di chi ha subito e, ancora una volta, ciò riduce fortemente l'empatia e il riconoscimento del danno provocato.

Sempre più spesso il cyberbullismo è collegato al bullismo tradizionale e ne diventa una specie di estensione: azioni di bullismo reale possono per esempio essere fotografate o videoriprese, per poi essere pubblicate e diffuse sul web (social network, siti di foto-video sharing, email, blog, forum e chat).

4.3 Hate speech: che cos'è e come prevenirlo

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

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

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

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

problematica.

Prevenire e/o contrastare: per riuscire a far emergere l' "hate speech" l'istituto "Tartaglia-Olivieri" propone annualmente una serie di attività che mirano all'Inclusione della diversità ed al rispetto con la creazione di un ambiente che favorisca la relazione tra pari, così come percorsi di Educazione Civica integrata all'e-safety sulla salvaguardia dei diritti dell'uomo e del fanciullo.

4.4 Dipendenza da Internet e gioco online

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

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

Tale dipendenza può manifestarsi anche attraverso le ore trascorse online a giocare e 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.

I segnali patologici di questo che viene descritto come "un vero e proprio abuso della tecnologia", anche denominato "Internet Addiction Disorder" (I.A.D. coniato dallo psichiatra Ivan Goldberg 1996), sono (così come accade per le altre dipendenze più "tradizionali"), in particolare, la tolleranza (crescente bisogno di aumentare il tempo su internet) e l'astinenza (l'interruzione o la riduzione dell'uso della Rete comportano ansia, agitazione psicomotoria, fantasie, pensieri ossessivi). Tutto questo ha ripercussioni sulla sfera delle relazioni interpersonali che diventano via via più povere e alle quali si preferisce il mondo virtuale, con alterazioni dell'umore e della percezione del tempo.

La S.I.I.Pa.C., Società Italiana Intervento Patologie Compulsive, definisce la dipendenza da Internet come progressivo e totale assorbimento del soggetto alla Rete; alcune caratteristiche specifiche sono:

- **Dominanza**: l'attività domina i pensieri ed il comportamento del soggetto, assumendo un valore primario tra tutti gli interessi.
- **Alterazioni del tono dell'umore**: l'inizio dell'attività provoca cambiamenti nel tono dell'umore. Il soggetto prova un aumento d'eccitazione o maggiore rilassatezza come diretta conseguenza dell'incontro con l'oggetto della dipendenza.
- **Conflitto**: conflitti interpersonali tra il soggetto e coloro che gli sono vicini, conflitti intrapersonali interni a se stesso, a causa del comportamento dipendente.
- **Ricaduta**: tendenza a ricominciare l'attività dopo averla interrotta.

Per poter parlare di patologia, si devono rilevare i seguenti comportamenti per almeno un anno:

- ✓ il giocatore è assorbito totalmente dal gioco;
- ✓ il giocatore è preoccupato e ossessionato dal gioco;
- ✓ il gioco consente alla persona di sfuggire alla realtà con la sperimentazione di emozioni più piacevoli;
- ✓ il giocatore manifesta sempre di più l'impulso di giocare e di sperimentare emozioni positive;
- ✓ il giocatore sente di dover dedicare più tempo ai giochi;
- ✓ il giocatore se non può giocare manifesta ansia, depressione e irritabilità;

- ✓ può emergere un ritiro sociale;
- ✓ il giocatore, anche se comprende la gravità della situazione e sospende di giocare comunque non riesce a interrompere del tutto;
- ✓ il giocatore mente agli altri sull'utilizzo che fa dei giochi on line;
- ✓ il giocatore ha perso o mette a rischio relazioni o opportunità a causa dei giochi su Internet o ha perso interesse verso attività nella vita reale.

L'istituzione scolastica nel suo ruolo educativo fornisce informazioni sulle varie tipologie di gioco on line e attua una prevenzione attraverso l'informazione e l'educazione dell'alunno all'uso consapevole di tutte le attività di gioco intese come momento di serenità e svago.

4.5 Sexting

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

Il "sexting" è un fenomeno molto frequente fra i giovanissimi, i quali inviano/ricevono contenuti mediali sessualmente espliciti senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video. Questi contenuti possono diventare materiale di ricatto assumendo la forma di "revenge porn" (letteralmente "vendetta porno"), fenomeno che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte (la Legge 19 luglio 2019 n. 69, all'articolo 10 ha introdotto in Italia il reato di revenge porn, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti. Si veda l'articolo 612 ter del codice penale rubricato "Diffusione illecita di immagini o video sessualmente espliciti"). Tra le caratteristiche del fenomeno vi sono principalmente:

- la fiducia tradita: chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo, inoltre, alla motivazione della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale);
- la pervasività con cui si diffondono i contenuti: in pochi istanti e attraverso una condivisione che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso a un numero esponenziale e infinito di persone e ad altrettante piattaforme differenti; il contenuto, così, diventa facilmente modificabile, scaricabile e condivisibile e la sua trasmissione è incontrollabile;
- la persistenza del fenomeno: il materiale pubblicato online può permanervi per un tempo illimitato e potrebbe non essere mai definitivamente rimosso. Un contenuto ricevuto, infatti, può essere salvato, a sua volta re-inoltrato oppure condiviso su piattaforme diverse da quelle originarie e/o in epoche successive.

La consapevolezza, o comunque la sola idea di diffusione di contenuti personali, si replica nel tempo e può finire con il danneggiare, sia in termini psicologici che sociali, sia il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che hanno contribuito a diffonderla. Due agiti, quindi, che sono fra loro

strettamente legati e che rappresentano veri e propri comportamenti criminali i quali hanno ripercussioni negative di chi ha subito in termini di autostima, di credibilità, di reputazione sociale off e on line. A ciò si associano altri comportamenti a rischio, di tipo sessuale ma anche riferibili ad abuso di sostanze o di alcool. I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/i e depressione.

4.6 Adescamento online

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

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

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

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

Sensibilizzare per contrastare tale fenomeno, capire inoltre il giovane e anticipare culturalmente il fenomeno. Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente. È importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che va compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e della sessualità. Fondamentale, inoltre, è portare avanti un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online.

4.7 Pedopornografia

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

La legge n. 269 del 3 agosto 1998 *"Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella* ***legge n. 38 del 6 febbraio 2006*** *"Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet"*, segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

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

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

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

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

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

La pedopornografia è un reato perseguibile d'ufficio e, come tale, se la realtà scolastica ne viene a conoscenza deve effettuare la denuncia all'autorità giudiziaria competente e garantire all'alunno, vittima di reato, il supporto psicologico. In particolare il personale docente e in generale il personale scolastico, in presenza di reati perseguibili di ufficio, deve riferire al dirigente scolastico la notizia di reato di cui è venuto a conoscenza nell'esercizio delle sue funzioni. Spetterà poi al Drigente scolastico l'obbligo di denunciare la notizia di reato all'autorità giudiziaria competente.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023).

□ Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.

□ Promuovere incontri i per studenti e studentesse dedicati all' Educazione Civica Digitale.

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).

□ Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.

□ Promuovere incontri per studenti e studentesse dedicati all' Educazione Civica Digitale.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. Cosa segnalare

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

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire).

Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).

Nelle procedure:

- sono indicate le figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso.
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

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

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

Tali procedure sono comunicate e condivise con l'intera comunità scolastica.

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

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

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

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

- Adescamento online: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- Sexting: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

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

La gestione dei casi rilevati va differenziata a seconda della loro gravità; fermo restando che è opportuna la condivisione a livello di Consiglio di Classe di ogni episodio, anche minimo, alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe. Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e come rimediare. Nei casi più gravi e in ogni ipotesi di reato occorre riferire tempestivamente al Dirigente Scolastico.

Come scuola vanno rilevati i: i comportamenti prepotenti e/o tutti quei comportamentii che hanno come obiettivo quello di danneggiare qualcuno in modo verbale, fisico o psicologico; gli elementi e materiali di vario genere postate in chat o social network; i contenuti che possano considerarsi in qualche modo lesivi: dell'onore, della reputazione e dell'immagine altrui; tutto ciò che rientra nella sfera sessuale: messaggi, immagini o video a sfondo sessuale.

5.2. Come segnalare: quali strumenti e a chi

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

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

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

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

Per tutti i dettagli fate riferimento agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

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

Per tutti i dettagli fate riferimento agli allegati con le procedure.

5.3. Gli attori sul territorio

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

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

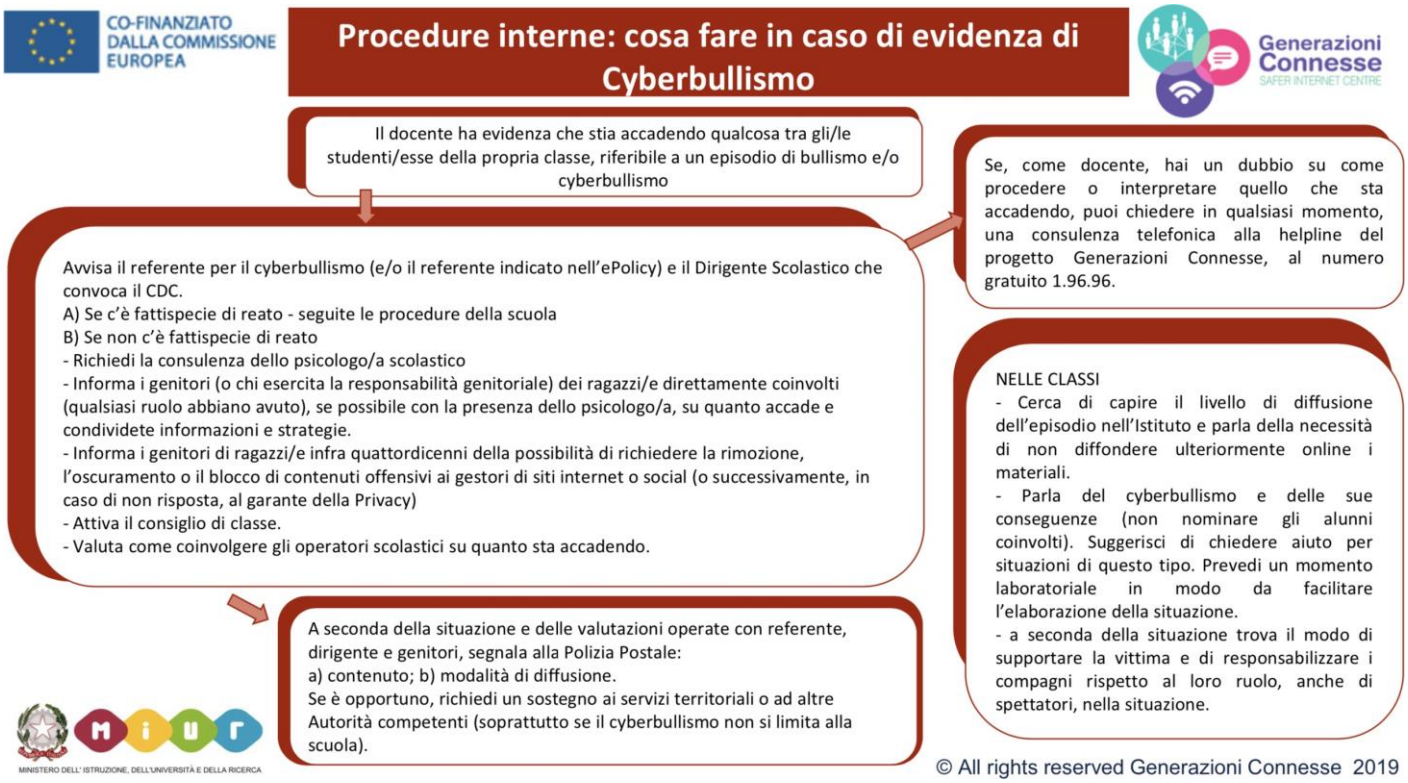
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

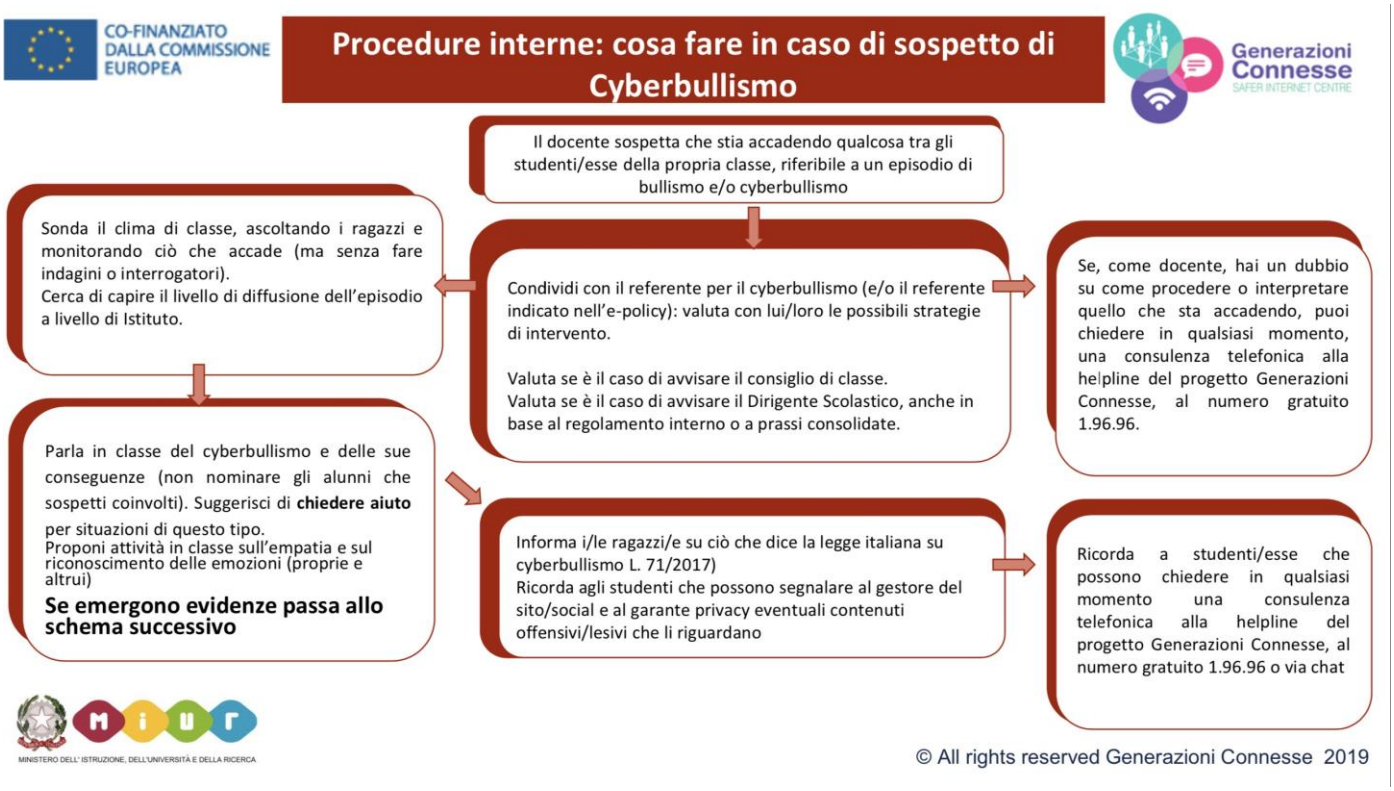
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com.** (Comitato Regionale per le Comunicazioni): svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.

- **Polizia Postale e delle Comunicazioni**: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti**: accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

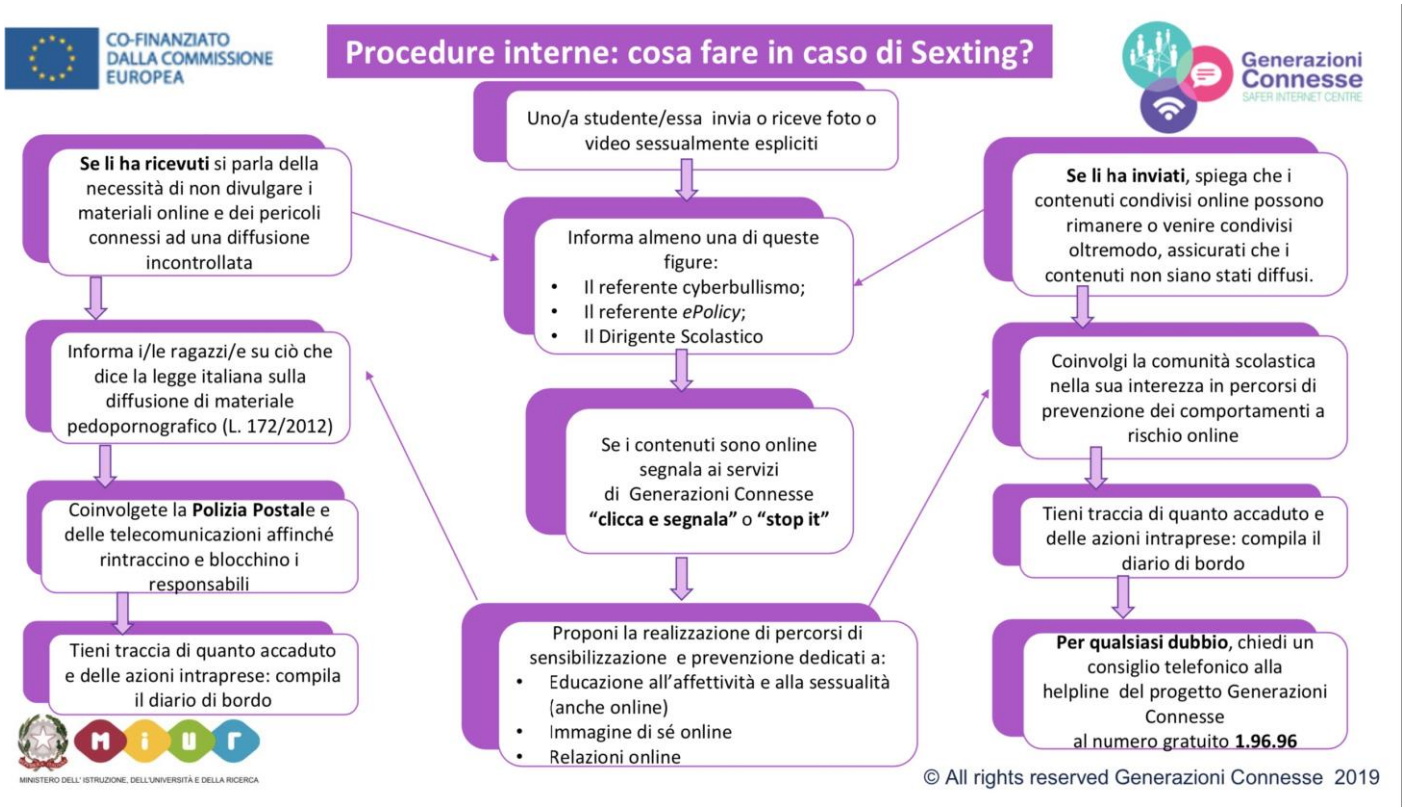
5.4. Allegati con le procedure

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

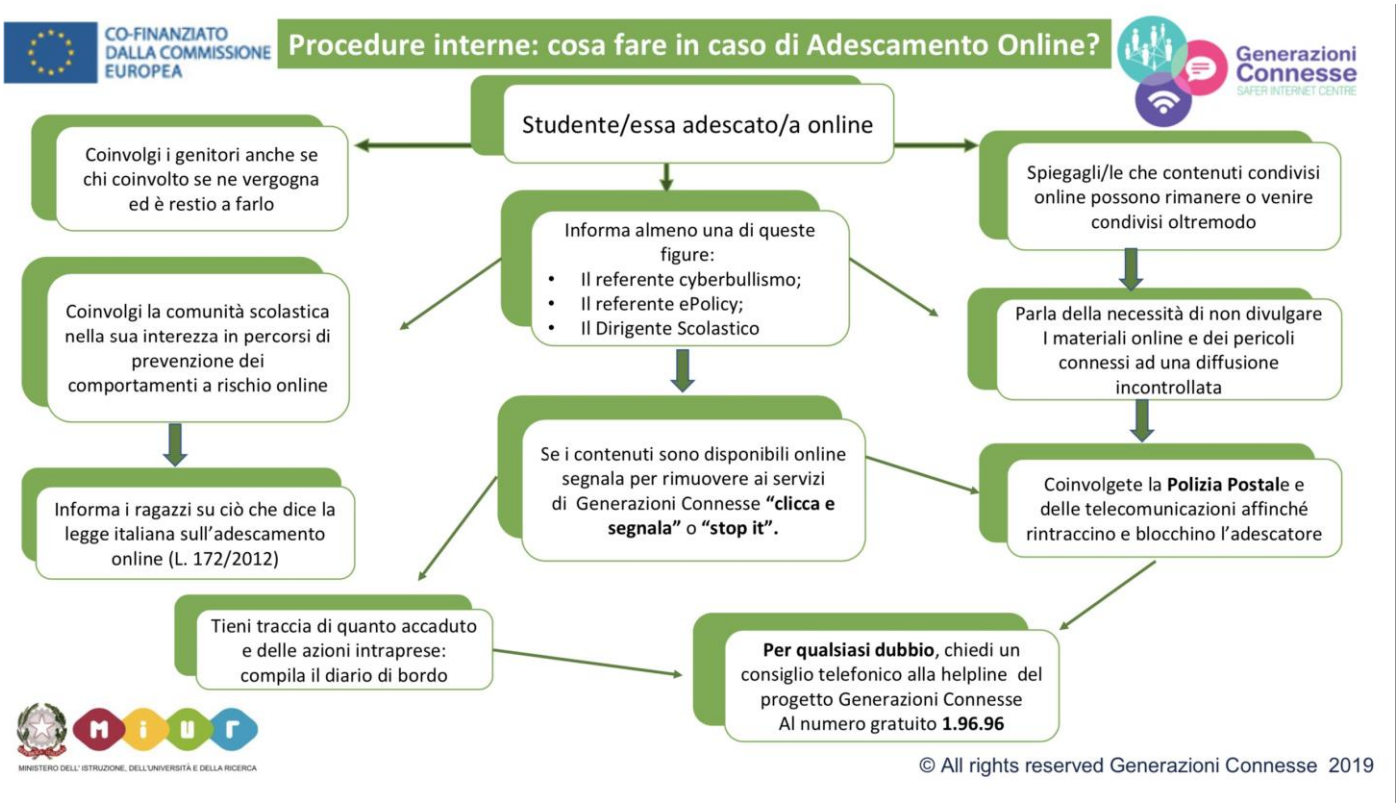



CO-FINANZIATO DALLA COMMISSIONE EUROPEA
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo
Generazioni Connesse
SAFER INTERNET CENTRE
Il docente sospetta che stia accadendo qualcosa tra gli studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo
Sonda il clima di classe, ascoltando i ragazzi e monitorando ciò che accade (ma senza fare indagini o interrogatori).
Cerca di capire il livello di diffusione dell'episodio a livello di Istituto.
Condividi con il referente per il cyberbullismo (e/o il referente indicato nell'e-policy): valuta con lui/loro le possibili strategie di intervento.
Valuta se è il caso di avvisare il consiglio di classe.
Valuta se è il caso di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.
Parla in classe del cyberbullismo e delle sue conseguenze (non nominare gli alunni che sospetti coinvolti). Suggerisci di chiedere aiuto per situazioni di questo tipo.
Proponi attività in classe sull'empatia e sul riconoscimento delle emozioni (proprie e altrui)
Se emergono evidenze passa allo schema successivo
Informa i/le ragazzi/e su ciò che dice la legge italiana su cyberbullismo L. 71/2017)
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano
Ricorda a studenti/esse che possono chiedere in qualsiasi momento una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 o via chat
MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
© All rights reserved Generazioni Connesse 2019

Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



Allegato 1 SCHEDA DI PRIMA SEGNALAZIONE

COGNOME E NOME DI CHI COMPILA LA SEGNALAZIONE

Istittuto_____Data_____

La persona che ha segnalato il caso era:

A

Chi ha subito

1. ❑ un compagno/a di chi ha subito (Cognome e nome: _____)
2. ❑ Madre/Padre/Tutore di chi ha subito (Cognome e nome: _____)
3. ❑ Insegnante (Cognome e nome: _____)
4. ❑ Altri (specificare):

B Chi ha subito

Cognome Nome _____classe_____
Cognome Nome _____classe_____
Cognome Nome _____classe_____

C Chia ha agito

Cognome Nome _____classe_____
Cognome Nome _____classe_____
Cognome Nome _____classe_____

Breve descrizione del problema presentato (Dare esempi concreti degli episodi di prepotenza facendo anche riferimento alla frequenza con cui sono avvenuti o avvengono

_____
_____
_____

allegato 2 SCHEDA DI VALUTAZIONE APPROFONTIDA

COGNOME E NOME DI CHI COMPILA LO SCREENING: _____

ISTITUTO: _____ DATA: _____

1. Data della segnalazione del caso: _____
2. La persona che ha segnalato il caso era:
   - ❑ Chi ha subito
   - ❑ un compagno/a di chi ha subito (Cognome e nome: _____)
   - ❑ Madre/Padre/Tutore di chi ha subito (Cognome e nome: _____)
   - ❑ Insegnante (Cognome e nome: _____)
   - ❑ Altri (specificare): _____
3. Cognome, Nome e ruolo della persona della scuola che ha compilato o che ha raccolto la prima segnalazione: _____
4. Chi ha subito?

   Cognome e nome _____ Classe: _____
   Cognome e nome: _____ Classe: _____
   Cognome e nome: _____ Classe: _____

5. Chi ha agito?

   Cognome e nome _____ Classe: _____
   Cognome e nome: _____ Classe: _____
   Cognome e nome: _____ Classe: _____

6. Che tipo di prepotenze sono accadute? Dare esempi concreti degli episodi.

   _____
   _____
   _____

7. In base alle informazioni raccolte, che cosa è avvenuto?
   1. è stato offeso, ridicolizzato e preso in giro in modo offensivo
   2. è stato ignorato completamente o escluso dal suo gruppo di amici
   3. è stato picchiato, ha ricevuto dei calci o è stato spintonato
   4. sono state messe in giro bugie/voci che hanno portato gli altri ad "odiarlo"
   5. gli sono stati presi dei soldi o altri effetti personali (o sono stati rotti)
   6. è stato minacciato o obbligato a fare certe cose che non voleva fare
   7. gli hanno dato dei brutti nomi, hanno fatto brutti commenti o gesti sulla sua etnia, colore della pelle, religione, orientamento sessuale, o identità di genere

8 ha subito delle offese o molestie sessuali attraverso parole, gesti o atti

9 è stato escluso da chat di gruppo, da gruppi Whatsapp o da gruppi online ha subito prepotenze online tramite computer o smartphone con messaggi offensivi, post o fotografie su Facebook, Whatsapp, Twitter, Myspace, Snapchat o tramite altri social media subito appropriazione di informazioni personali e utilizzo sotto falsa identità della propria password, account (email, Facebook, …) rubrica del cellulare;

10 Altro:_____

8. Quante volte sono successi gli episodi? _____

9. Quando è successo l'ultimo episodio

_____

10. Da quanto tempo si verificano questi episodi? _____

11. Si sono verificati episodi anche negli anni precedenti?

_____

_____

12.SOFFERENZA DI CHI HA SUBITO

Chi ha subito presenta	1NON VERO	2 QUALCHE VOLTA VERO	3 SPESSO VERO
Cambiamenti rispetto a com'era prima			
Ferite o dolori fisici non spiegabili			
Paura di andare a scuola (non va volentieri)			
Paura di prendere l'autobus - richiesta di essere accompagnato - richiesta di fare una strada diversa			
Difficoltà a relazionarsi con i compagni			
Isolamento/Rifiuto			
Bassa autostima			
Cambiamento nell'umore generale (è più triste, depressa, sola/ritirata)			
Manifestazioni di disagio fisico-comportamentale (mal di testa, mal di pancia, non mangia, non dorme,...)			
ha subito appropriazione di informazioni personali e utilizzo sotto falsa identità della propria password, account			

GRAVITÀ SITUAZIONE

PRESENZA DI TUTTE LE RISPOSTE CON LIVELLO 1	PRESENZA DI ALMENO UNA RISPOSTA CON LIVELLO 2	PRESENZA DI ALMENO UNA RISPOSTA CON LIVELLO 3
VERDE	***GIALLO***	***ROSSO***

13 **SINTOMATOLOGIA DI CHI HA AGITO**

Chi ha agito presenta	**NON VERO**	**QUALCHE VOLTA VERO**	**SPESSO VERO**
Comportamenti di dominanza verso i pari			
Presa di mira dei compagni più deboli			
Uno status per cui gli altri hanno paura di lui/lei			
Mancanza di paura/preoccupazione per le conseguenze delle proprie azioni			
Assenza di sensi di colpa (se rimproverato non mostra rimorso)			
Comportamenti che creano pericolo per gli altri			
Cambiamenti notati dalla famiglia			

GRAVITÀ SITUAZIONE

PRESENZA DI TUTTE LE RISPOSTE CON LIVELLO 1	PRESENZA DI ALMENO UNA RISPOSTA CON LIVELLO 2	PRESENZA DI ALMENO UNA RISPOSTA CON LIVELLO 3
VERDE	***GIALLO***	***ROSSO***

14 Da quanti compagni è sostenuto il soggetto che ha agito_____

15 Gli studenti che sostengono attivamente il soggetto che ha agito sono:

Cognome e nome _____ Classe: _____

Cognome e nome: _____ Classe: _____

Cognome e nome: _____ Classe: _____

16 Quanti compagni supportano il soggetto che ha subito o potrebbero farlo

_____

_____

17 Gli studenti che possono sostenere il soggetto che ha subito sono**:**

Cognome e nome _____ Classe: _____

Cognome e nome: _____ Classe: _____

Cognome e nome: _____ Classe: _____

18 Gli insegnanti sono intervenuti in qualche modo

_____

19 La famiglia o altri adulti hanno cercato di intervenire? Se sì, spiegare cosa è stato fatto

_____

20 La famiglia ha chiesto aiuto**?**

_____

_____

Il nostro piano d'azioni

AZIONI DA INTRAPRENDERE IN BASE AL LIVELLO DI RISCHIO:

DALLA VALUTAZIONE DELLA GRAVITA' ALLA SCELTA DI INTERVENTO:

1. **CODICE VERDE: LIVELLO DI RISCHIO BASSO**

- **AZIONI: Situazione da monitorare con interventi preventivi nella classe.**

1. **CODICE GIALLO: LIVELLO DI RISCHIO MEDIO**

AZIONI: interventi indicati e strutturati a scuola e in sequenza e
- **coinvolgimento della rete se *NON CI SONO RISULTATI***

1. ***CODICE ROSSO: LIVELLO DI RISCHIO ALTO***

AZIONI: Interventi di emergenza con supporto della rete

-