ISTITUTO DI ISTRUZIONE SUPERIORE
"LEONARDO DA VINCI"
Sedi Associate: Liceo - ITC
Segreteria didattica ☎ e 🖷 *0444/676125 – 670599*
Segreteria amministrativa ☎ *0444/672206 –* 🖷 *450895*
Via Fortis, 3 - 36071 Arzignano (VI)
C.F. 81000970244
e-mail: *viis00200@istruzione.it* – sito: *www.liceoarzignano.it*

E-Safety School Policy

ANNO SCOLASTICO1 2018-2019

INDICE

1.INTRODUZIONE	**3**
1.1 Ruoli e responsabilità	3
Il dirigente scolastico	4
Team dei collaboratori del dirigente	4
Decenti referenti – sportelli di ascolto	4
Animatore digitale	4
Il direttore dei servizi generali amministrativi	5
I docenti	5
Gli alunni	6
1.2. Condivisione e comunicazione della policy all'intera comunità	6
1.3 Gestione delle infrazioni alla policy	7
1.4. Monitoraggio dell'implementazione della policy e suo aggiornamento	8
2. FORMAZIONE E CURRICOLO	**9**
2.1. Curricolo sulle competenze digitali per gli studenti	9
2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle tic nella didattica	10
2.3. Formazione dei docenti sull' utilizzo consapevole e sicuro di Internet e delle tecnologie digitali	11
2.4. sensibilizzazione delle famiglie.	11
3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE TIC DELLA SCUOLA	**12**
3.1. Accesso a internet: filtro, antivirus e sulla navigazione	12
3.2. Gestione accessi (Password,Backup,ecc.).	13
3.3. E-mail	13
3.4. Sito web della scuola	13
3.5. Protezione dei dati personali	13
4. STRUMENTAZIONE PERSONALE	**14**
4.1. Per gli studenti gestione degli strumenti personali	14
4.2. Per i docenti gestione degli strumenti personali	15
5. PROTOCOLLO – RILEVAZIONE E GESTIONE DEI CASI	16
5.1. Definizione di bullismo e cyberbullismo	17
5.2. Cosa non è il bullismo	17
5.3. Rilevazione	18
5.4. Segnalazione (che cosa segnalare)	19
5.5. Come segnalare	19
5.6.Gestione dei casi	20
5.7. Prepotenza e prevaricazione	21
Scheda di Segnalazione in caso di presunto bullismo o prevaricazione	**23-24**
Procedura attuativa	**25-26**
Modello per la segnalazione di presunti casi di Bullismo e Cyberbullismo	27

1. INTRODUZIONE

Lo scopo della E-Policy è di presentare le linee guida dell'Istituto in merito all'utilizzo delle tecnologie dell'informazione. Tali tecnologie sono parte della regolare attività didattica nelle aule, sono utilizzate nella comunicazione scuola-famiglia e rivestono un ruolo importante nella vita sociale degli studenti. Data la pervasività di tali tecnologie, l'Istituto è chiamato non solo a redigere aspettative di comportamento alle quali tutti i membri della comunità scolastica sono chiamati ad attenersi, al fine di garantire un ambiente adeguato all'utenza e sicuro, ma anche ad attivare percorsi di formazione per promuovere un uso responsabile della rete. Opportune azioni disciplinari saranno intraprese nel caso di comportamenti inappropriati o addirittura illeciti. Affinché tali azioni risultino efficaci, è necessario il coinvolgimento di tutte le componenti della comunità scolastica, ognuno in relazione alla propria sfera di influenza. Con il presente protocollo pertanto si intende offrire a tutti gli attori coinvolti nel processo educativo, un supporto operativo che aiuti a prevenire e ad affrontare nel modo più adeguato le diverse situazioni legate ai fenomeni di bullismo e di cyberbullismo, in conformità con le linee di orientamento per azioni di prevenzione e di contrasto al bullismo e cyberbullismo legge n° 71/2017 elaborate dal MIUR in collaborazione con il Safer Internet Center per l'Italia, programma comunitario istituito dal Parlamento Europeo e dal Consiglio dell'Unione.

Vista l'importanza del tema, il documento potrà dunque, se necessario, essere modificato e aggiornato periodicamente in funzione di eventuali nuove esigenze e, di conseguenza, di nuove azioni da porre in essere anche nell'ottica di una sua piena integrazione con obiettivi e contenuti degli altri documenti di Istituto, primo tra tutti il PTOF.

1.1. RUOLI E RESPONSABILITÀ

La capacità di partecipare in modo costruttivo e consapevole alle comunità *on line* e ai network *virtuali* costituisce un prerequisito fondamentale per partecipare in modo attivo alla società della conoscenza e dell'informazione. Alla diffusione dei nuovi *media* e degli strumenti del *web 2.0-3.0* si accompagna infatti l'emergere di nuove opportunità di partecipazione civica e sociale (*engagement*, *e-inclusion*), che richiedono capacità comunicative e socio-relazionali adeguate. È fondamentale quindi conoscere come ci si comporta in queste comunità, quali regole vanno rispettate e quali ruoli e responsabilità hanno i soggetti che vi partecipano.

La scuola nel farsi carico della formazione globale del soggetto individuando in materia chiara e inequivocabili ruoli e responsabilità di ciascuno degli attori del percorso formativo.

Nella promozione dell'uso consapevole della rete:

AL DIRIGENTE SCOLASTICO:

Compete l'approvazione del presente documento e di ogni sua eventuale revisione, nonché la valutazione dell'efficacia, il monitoraggio, l'attività di indirizzo nell'attuazione della Policy, anche in collaborazione, oltre che con i docenti, con il personale scolastico, gli Enti Territoriali, le famiglie.

- **Favorire** la corretta formazione del personale scolastico sulle tematiche relative all'uso sicuro e consapevole di Internet e della rete;
- **Promuovere** una formazione adeguata del personale docente relativo all'uso TIC nella didattica;
- **Controllare** che le modalità di utilizzo corretto e sicuro delle TIC e di INTERNET siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- **Garantire** l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on line;
- **Seguire** le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola;

TEAM DI COLLABORATORI DEL DIRIGENTE:

Partecipano delle attività di salvaguardia della presente policy incentivando la riflessione e la progettazione in ottemperanza alle regole qui definite ed offrendo spunti per la sua integrazione e aggiornamento.

AI DOCENTI REFERENTI (SPORTELLI DI ASCOLTO)
PER LE AZIONI DI CONTRASTO AI FENOMENI DI BULLISMO/CYBER-BULLISMO

- **Compete** la stesura materiale e la revisione della policy sulla base delle osservazioni pervenute da tutti i soggetti dell'Istituzione scolastica;
- **Monitora** i fenomeni, costruendo strategie di intervento di rete;
- **Implementa** il team di supporto dei pari;
- **Offre** uno spazio di consulenza/supporto attraverso la creazione di sportelli tenendo rapporti con utenti esterni ed interni;
- **Avverte** tempestivamente la dirigenza per eventuali segnalazioni;
- **Organizza** uno o più incontri dedicati alla prevenzione dei rischi associati all'utilizzo di internet e delle tecnologie digitali, rivolte agli studenti, con il coinvolgimento delle famiglie.

ANIMATORE DIGITALE

Supportato dal *team* dell'innovazione tecnologica deve:

- **Stimolare** la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi *on line* e alle misure di prevenzione e gestione degli stessi;
- **Monitorare** e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché propone la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- **Coinvolgere** la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti alla "scuola digitale".

IL DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI DEVE:

- **Assicurare**, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;
- **Garantire** il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del dirigente scolastico e dell'animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.

I DOCENTI:

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

- **Informarsi/aggiornarsi** sulla politica della sicurezza adottata dalla scuola, rispettandone il regolamento;
- **Garantire** che le modalità di utilizzo corretto e sicuro delle TIC e della rete internet siano ove possibile integrate nel *curriculum* di studio e nelle attività didattiche ed educative delle classi;
- **Favorire** la comprensione da parte degli alunni delle regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;
- **Assicurare** che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
- **Garantire** che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi di comunicazione ufficiali;
- **Assicurare** la riservatezza dei dati personali trattati ai sensi della normativa vigente; controllare l'uso delle tecnologie digitali, dispositivi mobili, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito); nelle lezioni in cui è programmato l'utilizzo di internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su internet siano trovati e trattati solo materiali idonei;
- **Comunicare** ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di **approfondire** e concordare coerenti linee di intervento di carattere educativo;
- **Segnalare** qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo all'animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- **Segnalare** al dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.

GLI ALUNNI DEVONO:

- Leggere, comprendere e accettare la E-Safety Policy;
- Essere responsabili, in relazione alla propria età nell'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti e seguire scrupolosamente le indicazioni ricevute in merito all'utilizzo delle TIC;

- **Avere** una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali;
- **Comprendere** l'importanza di adottare buone pratiche di sicurezza on line quando si utilizzano le tecnologie digitali per non correre rischi.
- **Evitare il plagio**, rispettare le normative sul diritto d'autore, non diffondere dati personali;
- **Capire** le politiche di utilizzo delle immagini ed essere consapevoli del significato e della gravità del cyber-bullismo;
- **Esprimere** domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori;
- Negli spazi scolastici è fatto divieto di riprendere, scattare foto o effettuare registrazioni di eventi, fatti, situazioni o persone durante l'attività didattica senza espressa autorizzazione.

I GENITORI SONO TENUTI A:

- **Sostenere** la linea di condotta della scuola adottata nei confronti dell'utilizzo delle TIC nella didattica;
- **Seguire** gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti;
- **Concordare** con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet;
- **Fissare** delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e dello *smartphone* in generale.

1.2. CONDIVISIONE E COMUNICAZIONE DELLA POLICY ALL'INTERA COMUNITÀ SCOLASTICA

La scuola dovrà assicurare promozione della condivisione degli intenti esplicitati nel documento attraverso:

- Pubblicazione sul sito della scuola, sia all'interno della sezione dei regolamenti che di quella destinata al bullismo e al cyberbullismo.

CORPO DOCENTE:

- Approvazione a livello collegiale;
- Confronto collegiale, periodico, circa la necessità di apportare modifiche e miglioramenti alla policy vigente;
- Elaborazione di protocolli condivisi di intervento (**Cf. allegati del documento**).

COMPONENTE STUDENTESCA:

- Conoscenza del documento "Policy" nei primi giorni di scuola, da inserire anche nel progetto di accoglienza per le nuove classi prime;
- Inserimento di un estratto di questo documento nel diario scolastico con l'indicazione dei comportamenti corretti e di quelli da evitare.

GENITORI:

- Organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica;
- Informazione e formazione circa i comportamenti da monitorare e/o da evitare;

- Genitori esperti potranno collaborare nelle attività di informazione/formazione del personale e degli alunni.

1.3. GESTIONE DELLE INFRAZIONI ALLA POLICY

Le potenziali infrazioni a carico degli alunni sono identificabili in:

- Uso di *social network* e *altri social* per pubblicare, condividere o, in genere, postare commenti o giudizi offensivi della dignità altrui;
- Uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;
- Condivisione di dati personali che possano permettere l'accesso a dati sensibili;
- Connessioni a siti illegali o comunque non autorizzati;
- Pubblicazione di foto o immagini non autorizzate e/o compromettenti;
- Comunicazione incauta e senza permesso con gli sconosciuti;
- Condivisione di immagini intime o spinte;

Gli interventi educativi previsti per gli alunni sono rapportati a seconda della gravità e coerente con quanto definito nel regolamento di istituto.

La scuola eroga delle sanzioni secondo il principio della sensibilizzazione e del risarcimento dell'eventuale danno provocato, in uno spirito educativo.

Un primo intervento viene attuato dal docente/consiglio di classe secondo le modalità indicate:

- Richiamo verbale;
- Richiamo verbale con annotazione disciplinare sul registro e sul diario personale;
- Convocazione della famiglia.
- Sospensione dalle lezioni con lavori socialmente utili;
- Intervento degli organi competenti come previsto dalla legge 71/2017.

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

Le potenziali infrazioni a carico del personale scolastico sono identificabili in:

- Utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento, al profilo professionale, e che non abbiano finalità educative anche tramite l'installazione di *software* o il salvataggio di materiali non idonei;
- Trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della *privacy* o che non garantisce un'adeguata protezione degli stessi;
- Diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- Vigilanza elusa degli alunni durante le attività didattiche che può favorire un utilizzo non autorizzato delle TIC.

Il dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, come l'accesso a INTERNET, ma non alla posta elettronica personale.

Tutto il personale è tenuto a collaborare con il dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo gestionale, disciplinare amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse.

Disciplina dei genitori

In considerazione dell'età degli studenti, le azioni e la condotta dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola.

Le situazioni meno favorevoli sono:

- una piena autonomia concessa al proprio figlio nella navigazione sul *web* e nell'utilizzo dello *smartphone*;
- una posizione del *computer* in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio;
- 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 sanzionatorie anche a norma di legge.

1.4. MONITORAGGIO DELL'IMPLEMENTAZIONE DELLA POLICY E SUO AGGIORNAMENTO

Il monitoraggio dell'implementazione della policy e del suo eventuale aggiornamento sarà curato dal dirigente scolastico con la collaborazione dell'animatore digitale. Sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di INTERNET. Il monitoraggio sarà rivolto anche ai docenti, al fine di valutare l'impatto della policy e la necessità di eventuali miglioramenti. L'aggiornamento della policy sarà curato dal dirigente scolastico, dall' animatore digitale, dagli organi collegiali, a seconda degli aspetti considerati.

2. FORMAZIONE E CURRICOLO

L'impiego delle TIC è senz'altro un fattore di innovazione della didattica, di aumento della motivazione e del rendimento degli studenti. Tuttavia non è possibile risolvere una questione di tipo didattico esclusivamente su un piano tecnologico. È, invece, auspicabile una modifica delle pratiche tradizionali di insegnamento, infatti non è più sufficiente possedere la dotazione tecnologica, ma è fondamentale l'effettivo utilizzo che ne viene fatto, e quindi la capacità di comprenderne le potenzialità rispetto a contesti e finalità specifici.

Per sostenere questo processo all'interno della scuola è necessario investire sulla formazione e l'aggiornamento degli insegnanti, soprattutto in relazione alla didattica per competenze.

2.1. CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI

Il concetto di didattica per competenze ha assunto un ruolo centrale in ambito europeo. Nel 2006, il Parlamento Europeo ha elaborato una Raccomandazione (2006/962/CE) in cui delinea il quadro delle competenze necessarie per il *lifelong learning*, ovvero competenze necessarie per esercitare pienamente il diritto di cittadinanza nella società contemporanea. L'Italia ha progressivamente recepito il quadro comunitario dando vita a un processo di riforma educativa. Il tema della competenza digitale (*digital literacy*) è emerso all'interno del dibattito internazionale sul *lifelong learning*, ovvero sulla definizione dei saperi chiave per vivere attivamente nella cosiddetta società dell'informazione, un contesto che richiede un nuovo modello di alfabetizzazione in cui le nuove tecnologie e la rete possono essere considerati veri e propri vettori di partecipazione e la competenza digitale è quindi annoverata tra i sapere necessari per la cittadinanza.

Ma cosa significa essere competenti quando parliamo di TIC? Istintivamente si pensa ad abilità informatiche di base quali saper utilizzare il *computer*, conoscere specifici *software* o servizi *web*, possedere uno *smartphone*. Tuttavia, se proviamo a rispondere alla stessa domanda ponendoci in un'ottica pedagogica e partecipativa, penseremo probabilmente anche ad altre capacità come quella di saper cercare e selezionare le informazioni *online* in modo critico oppure saper lavorare in maniera collaborativa a distanza, tutelare la propria *privacy* nei *social network* e altre ancora. Questo semplice esercizio - che potremmo ripetere anche in classe con i nostri studenti - ci porta a considerare riduttiva una definizione di *digital literacy* come *expertise* tecnica, mettendo in luce le implicazioni cognitive e relazionali: diventa opportuno pensare la competenza digitale come un costrutto complesso, in cui si intersecano dimensioni di natura diversa, che potremmo così schematizzare:

- **Dimensione tecnologica**: questo ambito fa riferimento a una serie di *skills* tecnologiche di base, come ad esempio la conoscenza di dispositivi e interfacce, ma comprende anche livelli più

avanzati legati alla capacità di valutare le potenzialità dei contesti tecnologici in trasformazione, imparando a selezionare le soluzioni più opportune per affrontare ciascun compito;

- **Dimensione cognitiva**: comprende abilità legate al trattamento dell'informazione, dalla capacità di accedere, selezionare e interpretare dati a quella di valutarne criticamente la pertinenza e l'affidabilità, ma anche il saper trattare testi e dati per produrne sintesi, analisi e rappresentazioni con tabelle e grafici;
- **Dimensione etica**: questa dimensione riguarda il saper interagire con gli altri in modo corretto e responsabile, la circolazione del sapere *on line* e il rispetto dei diritti di proprietà intellettuale, il tema dell'accessibilità e dell'inclusione. Comprende alcune delle tematiche più attuali rispetto al tema delle nuove tecnologie, dalla tutela della *privacy* al contrasto del fenomeno del *cyberbullismo*, e quelle che riguardano la dimensione relazionale ed affettiva dell'utilizzo di internet: il fatto di non vedersi e di non sentirsi direttamente, o di non entrare in contatto visivo, abbassa timidezze e inibizioni, per cui spesso nella comunicazione in rete si raggiungono elevati livelli di confidenza e intimità e a volte, di seduttività, proprio perché l'altro/a può essere uno sconosciuto e come tale, liberamente immaginato e idealizzato.

Dall' integrazione di queste tre principali dimensioni emerge un concetto di competenza digitale che fa riferimento alla capacità di comprendere e sfruttare l'effettivo potenziale delle tecnologie in ottica di costruzione di conoscenza e di promozione della partecipazione e dell'inclusione: il rapporto con le tecnologie digitali guarda così a forme di uso consapevole, critico e creativo.

2.2. FORMAZIONE DEI DOCENTI SULL'UTILIZZO E L'INTEGRAZIONE DELLE TIC NELLA DIDATTICA

La formazione dei docenti e del personale che opera nella scuola è un importante elemento di qualità nel servizio scolastico; essa rappresenta una leva strategica per lo sviluppo culturale dell'istituzione scolastica, per il necessario sostegno agli obiettivi di cambiamento e per un'efficace politica delle risorse umane.

Il Piano di formazione del personale docente recepisce le criticità emerse dal RAV, le istanze rivenienti dal PDM e le proposte indicate nel *Piano nazionale scuola digitale*.

Il percorso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica dovrebbe diventare un processo permanente e può prevedere anche momenti di autoaggiornamento.

2.3. FORMAZIONE DEI DOCENTI SULL'UTILIZZO CONSAPEVOLE E SICURO DI INTERNET E DELLE TECNOLOGIE DIGITALI

Coerentemente con quanto previsto dal PNSD, la nostra scuola può avvalersi dell'animatore digitale secondo quanto previsto dall' azione #28 che, di concerto con il Dirigente Scolastico e il D.S.G.A. avvia un ruolo strategico nella diffusione ed applicazione dell'innovazione.

Anche il percorso della formazione specifica dei docenti sull'utilizzo consapevole e sicuro di internet può prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi.

Per realizzare gli interventi previsti dal PNSD può scegliere di agire su due fronti:

- **Organizzare** corsi interni, sia predisposti dall'istituto che da scuole in rete, per favorire uno sviluppo professionale proattivo; con particolare attenzione alla promozione di approcci e culture nuove nei confronti del proprio ruolo e dei compiti ad esso connessi;
- **Favorire** la partecipazione a corsi esterni inerenti la didattica innovativa per ogni singola disciplina e/o che rispondano ad esigenze formative del sistema scolastico nel suo complesso.

Si farà ricorso, volta per volta e secondo le esigenze, alle risorse sotto indicate:

- Personale docente interno alla scuola che abbia acquisito competenze in determinati settori affini alle esigenze sopra evidenziate;
- Creazione di una rete di formazione tra scuole che operi con modalità di ricerca-azione e ponga in relazione le esperienze formative vissute con le azioni didattiche svolte in classe e la successiva riflessione attivata su di esse;
- Soggetti esterni che offrano la possibilità di mettere in opera un'attività di consulenza mediante seminari e incontri-dibattito;
- Formazione a distanza.

Sarà consentita la partecipazione ad iniziative al di fuori della pianificazione d'Istituto, in coerenza con le finalità e gli obiettivi del Piano.

2.4. SENSIBILIZZAZIONE DELLE FAMIGLIE

In considerazione dell'importanza di favorire la sinergia degli interventi educativi di scuola e famiglia per il successo scolastico ed educativo di ogni studente, il presente documento, assieme al *Patto educativo di corresponsabilità* stipulato con le famiglie degli alunni quale impegno reciproco di scuola e famiglia alla corresponsabilità formativa, nella quale rientrano a pieno titolo i temi legati alla *eSafety*, è a disposizione delle famiglie sul sito *web* d'Istituto.

Allo scopo di mantenere viva l'attenzione delle famiglie sui tali temi, verranno inoltre valorizzate le 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.
Il coinvolgimento dell'intera comunità scolastica è parte integrante del PTOF.
Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di *smartphone*, *chat line* e *social network* più diffusi, con particolare riferimento alla prevenzione del *cyberbullismo*. Si prevede la creazione di una bacheca virtuale sul sito scolastico istituzionale per la condivisione di materiali dedicati al tema del *web* sicuro.

3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE TIC DELLA SCUOLA

L'infrastruttura e la strumentazione TIC dell'istituto sono un patrimonio di tutti, esse vanno utilizzate nel rispetto delle norme contenute nel "Regolamento per l'utilizzo dei laboratori multimediali". danni causati alle attrezzature saranno a carico di chiunque disattenda il suddetto regolamento.
L'accesso ad infrastrutture e strumentazione TIC utilizzabili per la didattica è riservato ai docenti e agli alunni ed è limitato al perseguimento di scopi formativi. I docenti devono formare i propri alunni al rispetto del suddetto regolamento, per gli aspetti di loro pertinenza.
La scuola deve considerare l'ambiente *on line* alla stregua dell'ambiente fisico, e valutarne tutti gli aspetti legati alla sicurezza nel momento in cui permette l'accesso alla rete tramite i collegamenti scolastici.
L'aggiornamento delle infrastrutture permette l'accesso a internet a tutte le classi/laboratori, attraverso una rete WI-FI e/o cablata.

L'infrastruttura quindi non va più pensata solamente come *hardware* e rete (*wireless* e non), ma occorre anche considerare tutti gli aspetti che riguardano la gestione degli *account* degli utenti (in modo differenziato tra studenti e insegnanti), il filtraggio dei contenuti e gli aspetti legali che riguardano prevalentemente la *privacy*.

Per quanto concerne l'*hardware*, la scuola provvede a pianificare interventi periodici di manutenzione grazie ad una figura con incarico specifico relativo alla gestione/manutenzione delle apparecchiature. Per creare ambienti di apprendimento nei quali sia possibile collaborare, co-creare, interagire, ricercare documentazioni e risorse, progettare, ampliare l'orizzonte conoscitivo degli alunni, l'Istituto avvierà in alcune classi, l'impiego didattico del tablet e della "Flipped classroom" sempre nel rispetto delle scelte dei singoli consigli di classe e della libertà di insegnamento del singolo docente.

3.1. ACCESSO AD INTERNET: FILTRI, ANTIVIRUS E SULLA NAVIGAZIONE

L'accesso attraverso WI-FI è protetto. Tutti gli utenti sono dotati di *password personale*. Filtri installati sui *server* impediscono il collegamento a siti appartenenti alla *black list*.

Gli ultimi adeguamenti tecnologici hanno previsto il potenziamento della rete LAN/WLAN attraverso *access point*, apparati di rete *switch*, armadi *rack* a parete e *firewall*.

3.2. GESTIONE ACCESSI (PASSWORD, BACKUP, ECC.)

La scuola adotta tutte le necessarie precauzioni per evitare l'accesso a siti non adatti all'interno della scuola. Questo avviene attraverso l'adozione di *apposite protezioni Firewall e black list*.

L'accesso ai portali si effettua per mezzo di *password utente* uniche e personali.

I docenti possono accedere alla propria sezione del registro elettronico con credenziali personali. Anche a genitori e alunni sono state fornite credenziali personali di accesso al registro elettronico.

I dati personali vengono trattati nel rispetto della normativa sulla *privacy*.

3.3. E-MAIL

L'accesso alla posta elettronica istituzionale della scuola può essere effettuato solo dal personale di segreteria e dalla presidenza utilizzando credenziali uniche.

Il personale utilizza un'e-mail propria e univoca.

3.4. SITO WEB DELLA SCUOLA

La scuola è dotata di un sito istituzionale con estensione http://www.infoliceoleonardodavinci.it/ sul quale diversi siti tematici rimandano al contenuto di interesse (amministrazione trasparente, albo pretorio, circolari, bacheca sindacale ecc.). Per mezzo di credenziali personali si accede all'area riservata per la presa visione delle comunicazioni ufficiali indirizzate ai docenti, mentre le circolari sono consultabili liberamente. Sul sito è possibile trovare regolamenti, materiali didattici, pubblicizzazione di eventi, documentazione di attività curricolari ed extracurricolari svolte.

3.5. PROTEZIONE DEI DATI PERSONALI

Nell'epoca della condivisione, in cui il confine tra pubblico e privato sembra essere costantemente messo in discussione, è necessario imparare a gestire i propri dati sensibili e a tutelarli, anche alla luce delle strategie di *web marketing* e profilazione dell'utente. Per questo motivo 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).

Ai genitori viene fornita una informativa sul trattamento dei dati personali ai sensi dell'art. 13 del D. Lgs. 30 giugno 2003, n. 196 e successive, e richiesta di autorizzazione all'utilizzo dei dati personali degli. alunni eccedenti i trattamenti istituzionali obbligatori, come ad esempio l'utilizzo di fotografie, video o altri materiali audiovisivi contenenti l'immagine, il nome e la voce del proprio figlio/a, all'interno di

attività educative e didattiche per scopi documentativi, formativi e informativi, durante gli anni di frequenza della scuola

4.STRUMENTAZIONE PERSONALE

4.1. PER GLI STUDENTI GESTIONE DEGLI STRUMENTI PERSONALI .

Agli alunni è consentito portare il cellulare a scuola per motivi familiari e organizzativi. Coerentemente con quanto indicato dalla Direttiva Ministeriale n. 30 del 15 marzo 2007, gli studenti sono però tenuti a tenere il cellulare spento durante le lezioni. Tuttavia, qualora ritenuto opportuno dal docente, è previsto l'uso dei *personal device* degli studenti. Il Regolamento d'istituto viene pertanto aggiornato onde prevedere il BYOD.

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*. Inoltre, poiché gli smartphone possono essere utilizzati anche per scattare foto (o effettuare riprese filmate) e per trasferirle in rete, si ribadisce come tali fatti si possono configurare come reati per i quali non si esclude la segnalazione ai competenti organi di Pubblica Sicurezza.

L'Istituzione Scolastica non ha e comunque non si assume alcuna responsabilità né relativamente all'uso improprio o pericoloso che gli studenti dovessero fare del cellulare (es.: inviare/ricevere messaggi a/da soggetti ignoti agli stessi genitori), né relativamente a smarrimenti e/o furti di smartphone, tablet, di lettori mp3/4 o di memorie di massa portatili.

In ogni caso, le famiglie che necessitano di comunicazioni urgenti ed improcrastinabili possono rivolgersi alla segreteria.

Il divieto ribadito per i telefoni/smartphone e per i lettori si estende ovviamente anche ad altri oggetti il cui uso a scuola può persino arrecare danni a terzi.

La scuola non pone alcun ostacolo all'utilizzo di cd/dvd rom o di hard-disk portatili, tablet come strumenti di lavoro e di studio. Ciò che a riguardo compete alle famiglie è il controllo periodico del contenuto di questi strumenti per evitare che qualche studente 'trasporti' a scuola immagini/testi/filmati per così dire 'sconvenienti'.

Fermo restando il fatto che la scuola è un'istituzione educativa e che non è né prevista, né possibile, né tantomeno legittima la perquisizione quotidiana di tutti gli studenti all'inizio di ogni giorno di lezione, le responsabilità che dovessero derivare dal verificarsi di eventi riconducibili all'uso non corretto o non legittimo di uno qualsiasi degli oggetti di cui alla presente norma regolamentare sono tutte ascrivibili alle famiglie degli studenti eventualmente coinvolti.

4.2. PER I DOCENTI: GESTIONE DEGLI STRUMENTI PERSONALI

Durante le ore delle lezioni non è consentito l'utilizzo del cellulare o di altri device personali se non a scopo didattico ed integrativo di quelli scolastici disponibili.
Tutto il personale scolastico è autorizzato ad utilizzare device personali laddove non stia assolvendo ad un ruolo didattico, a condizione che l'utilizzo non intralci il normale svolgimento delle attività scolastiche, né distragga dal corretto svolgimento delle proprie mansioni. In tal caso la responsabilità sulla conservazione e corretta gestione degli stessi è affidata unicamente al proprietario.

5. PROTOCOLLO - RILEVAZIONE E GESTIONE DEI CASI PREVENZIONE

Poiché il bullismo e il cyberbullismo sono fenomeni complessi e articolati, è essenziale procedere ad una loro precisa definizione, indispensabile per riconoscerli e contrastarli. Il nostro intervento contro il bullismo è il comportamento prepotente tra ragazzi a scuola si connota, con la maggior parte degli interventi adottati in questi casi, per un approccio globale di tipo sistemico ed ecologico, che integra al suo interno diversi livelli di intervento, dalla scuola come sistema fino ai singoli individui coinvolti nel fenomeno, passando attraverso la classe e il gruppo.

L'assunto alla base di questo approccio è che il clima della scuola e le dinamiche interne ai gruppi-classe possano giocare un ruolo significativo al fine di potenziare o viceversa ridurre e prevenire il problema. Altro carattere distintivo del nostro intervento nel settore, riconducibile al modello ecologico, è l'idea di dover agire, per lo più, attivando le risorse della scuola stessa: insegnanti, studenti, genitori, personale non docente. L'obiettivo primario è che il fenomeno delle prepotenze tra ragazzi a scuola non rimanga pervaso da un clima di silenzio ed omertà, vista la difficoltà sussistente a riferire o a denunciare episodi accaduti da parte di coloro che subiscono i comportamenti aggressivi dei compagni.

5.1. DEFINIZIONE

Il bullismo è un fenomeno che generalmente si sviluppa all'insaputa dell'adulto, sia esso insegnante, genitore, personale non docente o dirigente scolastico e, pertanto, affinché l'azione di prevenzione possa risultare efficace, è importante il coinvolgimento di tutte queste figure, ognuna in relazione alla sfera di competenza.

Nell'ambito di tale fenomeno, peraltro, è fondamentale non trascurare quel particolare aspetto che va sotto il nome di cyberbullismo: il mondo digitale e virtuale, infatti, rappresenta un'enorme opportunità di sviluppo e di crescita culturale e sociale ma nasconde, però, una serie di insidie e pericoli cui occorre far fronte promuovendo sinergie creative tra le istituzioni, con l'obiettivo di accrescere e rafforzare il senso della legalità.

Le linee guida qui riportate rappresentano la volontà dell'Istituto Leonardo da Vinci di promuovere e migliorare il senso di benessere a scuola e di prevenire situazioni di disagio, quale quello del bullismo:

- **INTENZIONALITA**': il bullo mette in atto comportamenti fisici, verbali o psicologici con lo scopo di offendere l'altro e arrecargli danno e disagio;
- **PERSISTENZA**: la ripetività di comportamenti protratti nel tempo;
- **ASIMMETRIA** dell'interazione: disequilibrio e diseguaglianza di forza, tra il bullo che agisce e la vittima che non è in grado spesso di difendersi;
- l'attacco può essere DIRETTO : modalità fisiche o verbali (pugni, botte, offese..)

o INDIRETTO: di tipo psicologico (esclusione o diffamazione ...)

- CYBERBULLING: molestie attuate attraverso strumenti tecnologici.

5.2.COSA NON E' IL BULLISMO:

- REATO: Alcuni episodi (attacchi con armi, coltelli, furti, minacce di aggressione.) hanno una natura più severa; in questo caso sono dei veri e propri crimini e come tali vanno affrontati dalla polizia e dal tribunale dei minori;
- SCHERZO: Particolarmente frequenti nell'interazione tra studenti, anche se la situazione in alcuni casi può degenerare e diventare un vero attacco, spesso sono comportamenti di natura ludica.

I vissuti dei ragazzi coinvolti, pertanto, costituiscono i principali indicatori per l'individuazione di singole prepotenze e di situazioni di bullismo. Il cyberbullismo (ossia "bullismo" online) è il termine che indica atti di bullismo e di molestia effettuati tramite mezzi elettronici come l'e-mail, sms, i blog, smartphone e/o i siti web.

Per i ragazzi nativi digitali le interconnessioni tra vita e tecnologia sono la normalità.

Essi, pur essendo spesso tecnicamente competenti, tendono a non cogliere le implicazioni dei loro comportamenti e tale fenomeno è tanto maggiore quanto è più forte il coinvolgimento emotivo dell'utilizzo di tali strumenti.

Tra i principali rischi, sia di carattere comportamentale che di matrice tecnica, ricordiamo:

- Possibile esposizione a contenuti violenti e non adatti alla loro età;
- **FLAMING:** Litigi on line nei quali si fa uso di un linguaggio violento e volgare.
- **HARASSMENT**: molestie attuate attraverso l'invio ripetuto di linguaggi offensivi.
- **CYBERSTALKING**: invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la propria incolumità.
- **DENIGRAZIONE**: pubblicazione di pettegolezzi e commenti crudeli, calunniosi e denigratori all'interno di comunità virtuali, quali newsgroup, blog, forum di discussione,
- **OUTING ESTORTO**: registrazione delle confidenze - raccolte all'interno di un ambiente privato - creando un clima di fiducia e poi inserite integralmente in un blog;
- **IMPERSONIFICAZIONE**: insinuazione all'interno dell'account di un'altra persona con l'obiettivo di inviare dal medesimo messaggi ingiuriosi che screditino la vittima.
- **ESCLUSIONE:** estromissione intenzionale dall'attività on line.
- **SEXTING:** invio di messaggi via smartphone ed Internet, corredati da immagini a sfondo sessuale.
- **SEXTORTION**: pratica utilizzata dai cyber criminali per estorcere denaro, la vittima viene convinta a inviare foto e/o video osé e poi le si chiede un riscatto per non pubblicarle.
- Videogiochi diseducativi;

- Pubblicità ingannevoli;
- Virus informatici in grado di infettare computer e cellulari;
- Adescamento on line (grooming);
- Uso eccessivo di internet/smartphone (dipendenza);

  È opportuno che i docenti, nell'espletamento delle proprie funzioni di formatori ed educatori, sappiano cogliere ogni opportunità per riflettere insieme agli studenti su tali rischi. Fondamentale è monitorare costantemente le relazioni interne alla classe, onde individuare possibili situazioni di disagio ed intervenire tempestivamente, anche mediante il ricorso alle figure specializzate, per sostenere il singolo nelle situazioni di difficoltà personale e indirizzare il gruppo verso l'istaurazione di un clima positivo, di reciproca accettazione e rispetto, nelle situazioni di difficoltà socio-relazionale.

Tale percorso interno potrà essere ulteriormente rinforzato dalla partecipazione a progetti e/o iniziative esterne coerenti con i temi sopra menzionati, cui la scuola porrà particolare attenzione, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità.

5.3.RILEVAZIONE

L'Istituto Leonardo Da Vinci, prevede per l'anno scolastico 2018-2019 la figura di due referenti per il bullismo: la professoressa Breda Carla e per il cyberbullismo il prof. Montepaone Antonio.

È stato fornito agli studenti un indirizzo di posta elettronica attraverso cui segnalare atti di scorretto utilizzo della rete anche al fine di prevenire e contrastare il fenomeno del cyberbullismo. Inoltre, chiunque viene a conoscenza di comportamenti scorretti sulla rete può segnalarlo al dirigente scolastico attraverso la scheda di segnalazione allegata.

5.4.SEGNALAZIONE (CHE COSA SEGNALARE)

Gli alunni possono mostrare segni di tristezza o di ansia o di risentimento nei confronti di compagni o di altri e riferire spontaneamente o su richiesta l'accaduto ai docenti.

I fatti riferiti possono essere accaduti anche al di fuori della scuola. Anche confrontandosi periodicamente con gli alunni sui rischi delle comunicazioni online, i minori possono riferire di fatti o eventi personali o altrui che "allertano" l'insegnante.

Una "prova" di quanto riferito può essere presente nella memoria degli strumenti tecnologici utilizzati, può essere mostrata spontaneamente dall'alunno, può essere presentata da un reclamo dei genitori, può essere notata dall'insegnante che si accorge dell'infrazione in corso. Mentre il docente è autorizzato a controllare le strumentazioni della scuola, per controllare l'uso del telefono cellulare di un alunno si rivolge al genitore. I contenuti "pericolosi" comunicati/ricevuti a/da altri, messi/scaricati in rete, ovvero

le tracce che possono comprovare l'utilizzo incauto, scorretto o criminoso degli strumenti digitali utilizzabili anche a scuola attualmente dai minori (l'eventuale telefonino/smartphone personale e il pc collegato a Internet) per gli alunni possono essere i seguenti:

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

5.5. COME SEGNALARE: QUALI STRUMENTI E A CHI.

Per il telefono cellulare ci si può assicurare che l'alunno vittima salvi nel suo telefono ogni messaggio, voce/testo/immagine, conservando così il numero del mittente.

Gli insegnanti, anche con l'ausilio tecnico dell'animatore digitale, possono provvedere ugualmente a conservare le prove della condotta incauta, scorretta o dell'abuso rilevate sui pc della scuola: soprattutto la data e l'ora, il contenuto dei messaggi e, se possibile, l'ID del mittente (es. username, mail, numero di telefono cellulare) o l'indirizzo web del profilo ed il suo contenuto.

Qualora ci si dovesse accorgere che l'alunno, usando il computer, si sta servendo di un servizio di messaggeria istantanea, programma che permette di chattare in linea tramite testo, l'insegnante può copiare, incollare e stampare la conversazione.

Per gli eventuali collegamenti non autorizzati a siti social network, video-hosting sites e altri website, l'insegnante può conservare il link, stampare la pagina o salvare la schermata su documento word. Per le e-mail si può stampare la mail o conservare l'intero messaggio, compresa l'intestazione del mittente.

Conservare la prova è utile per far conoscere l'accaduto in base alla gravità ai genitori degli alunni, al dirigente scolastico e per le condotte criminose alla polizia. Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno, quantunque riferite a fatti accaduti al di fuori del contesto scolastico, le notizie raccolte sono comunque comunicate ai genitori e per fatti rilevanti anche al dirigente scolastico; per quelle criminose, anche alla polizia. In particolare la segnalazione viene fatta a entrambe le famiglie, se oltre alla vittima anche l'autore della condotta negativa è un altro alunno. Per le segnalazioni di fatti

rilevati sono previsti i seguenti strumenti che i docenti possono utilizzare sulla base della gravità dell'accaduto:

- Annotazione del comportamento sul registro e comunicazione scritta ai genitori, che la devono restituire vistata;
- Convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti;
- Relazione scritta al dirigente scolastico.

In base all'urgenza le comunicazioni formali possono essere precedute da quelle informali, effettuate per le vie brevi.

Inoltre per i reati meno gravi la legge rimette ai genitori degli alunni la scelta di richiedere la punizione del colpevole, attraverso la querela.

Per i reati più gravi (es. pedopornografia) gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti).

In particolare per i fatti criminosi, ai fini della denuncia, la relazione deve essere redatta nel modo più accurato possibile, indicando i seguenti elementi: il fatto, il giorno dell'acquisizione del fatto nonché le fonti di prova già note e per quanto possibile, le generalità, il domicilio e quant'altro di utile a identificare la persona alla quale il reato è attribuito, la persona offesa, e tutti coloro che sono in grado di riferire circostanze rilevanti per la ricostruzione del fatto.

5.6.Gestione dei casi

Definizione delle azioni da intraprendere a seconda della specifica del caso.

Gestione dei casi di "immaturità - ingenuità"

Può sembrare naturale all'alunno fornire i propri dati sui siti allestiti in modo tale da attrarre l'attenzione dei ragazzi, con giochi e animazioni, personaggi simpatici e divertenti, che richiedono una procedura di registrazione.

Curiosità, manifestazioni di reciproco interesse tra pari, idee e fantasie sulla sessualità sono espressione da una parte del progressivo sviluppo socio-affettivo dell'alunno e dall'altra dei molteplici messaggi espliciti che gli giungono quotidianamente attraverso i media (televisione, DVD, internet, giornali e riviste), i discorsi degli altri ragazzi o degli adulti.

I comportamenti cosiddetti "quasi aggressivi", che spesso si verificano tra coetanei, le interazioni animate o i contrasti verbali, o la presa in giro "per gioco", effettuata anche in rete, mettono alla prova la relazione con i compagni, la supremazia o la parità tra i soggetti implicati e l'alternanza e sperimentazione dei diversi ruoli. Il gruppo dei pari rappresenta anche il momento di conquista dell'autonomia dall'adulto e pertanto luogo di "complicità" e di piccole "trasgressioni", di scambi "confidenziali" condivisi fra gli amici nella rete o con il cellulare.

Detti comportamenti, che finiscono per arrivare all'attenzione degli adulti, sono controllati e contenuti dai docenti attraverso i normali interventi educativi, di richiamo al rispetto delle regole di convivenza civile e democratica, di rispetto degli altri, per evitare che possano degenerare, diventare pericolosi per sé o offensivi e minacciosi per gli altri.

Gestione dei casi di "prepotenza" o "prevaricazione"

I comportamenti definibili "bullismo" possono esprimersi nelle forme più varie e non sono tratteggiabili a priori; se non contestualizzandoli. Le caratteristiche che aiutano a individuarli e a distinguerli dallo scherzo, dalle intemperanze caratteriali, dai diverbi usuali fra i ragazzi sono la costanza nel tempo e la ripetitività, l' asimmetria (disuguaglianza di forza e di potere), il disagio della/e vittima/e. Il bullismo si esplica infatti con comportamenti e atteggiamenti costanti e ripetitivi di arroganza, prepotenza, prevaricazione, disprezzo, dileggio, emarginazione, esclusione ai danni di una o più persone, agiti da un solo soggetto, ma in genere da un gruppo.
Nel caso particolare del cyberbullismo le molestie sono attuate attraverso strumenti tecnologici:

- Invio di sms, messaggi in chat, e-mail offensive o di minaccia;
- Diffusione di messaggi offensivi ai danni della vittima, attraverso la divulgazione di sms o email nelle mailing-list o nelle chat-line;
- Pubblicazione nel cyberspazio di foto o filmati che ritraggono prepotenze o in cui la vittima viene denigrata.

Il bullismo in particolare può originarsi anche dall'esasperazione di conflitti presenti nel contesto scolastico. Il conflitto, presente in ogni normale intenzione, è da considerarsi come un campanello d'allarme e può degenerare in forme patologiche quando non lo si riconosce e gestisce in un'ottica evolutiva dei rapporti, di negoziazione e risoluzione. Se non gestito positivamente, infatti, il conflitto rischia di mutarsi e provocare effetti distruttivi sulle relazioni (prevaricazione e sofferenza) e sull'ambiente (alterazione del clima del gruppo-classe).
In considerazione dell'età degli alunni considerati possono prefigurarsi alcune forme di interazioni che possono evolvere verso tale fenomeno. Per prevenire e affrontare il bullismo dunque i docenti non solo identificano vittime e prepotenti in divenire, ma tutti insieme affrontano e intervengono sul gruppo-classe, coinvolgendo i genitori degli allievi.

L'elemento fondamentale per una buona riuscita dell'intervento educativo è infatti la corretta, compiuta e convinta ristrutturazione dell'ambiente sociale in cui tale fenomeno si verifica, e in particolare delle relazioni nel contesto della classe. Gli atteggiamenti degli alunni, così come quelli dei loro genitori, possono giocare un molto significativo nel ridurre la dimensione del fenomeno.
Gli interventi mirati sul gruppo classe sono gestiti in collaborazione dal team dei docenti della

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

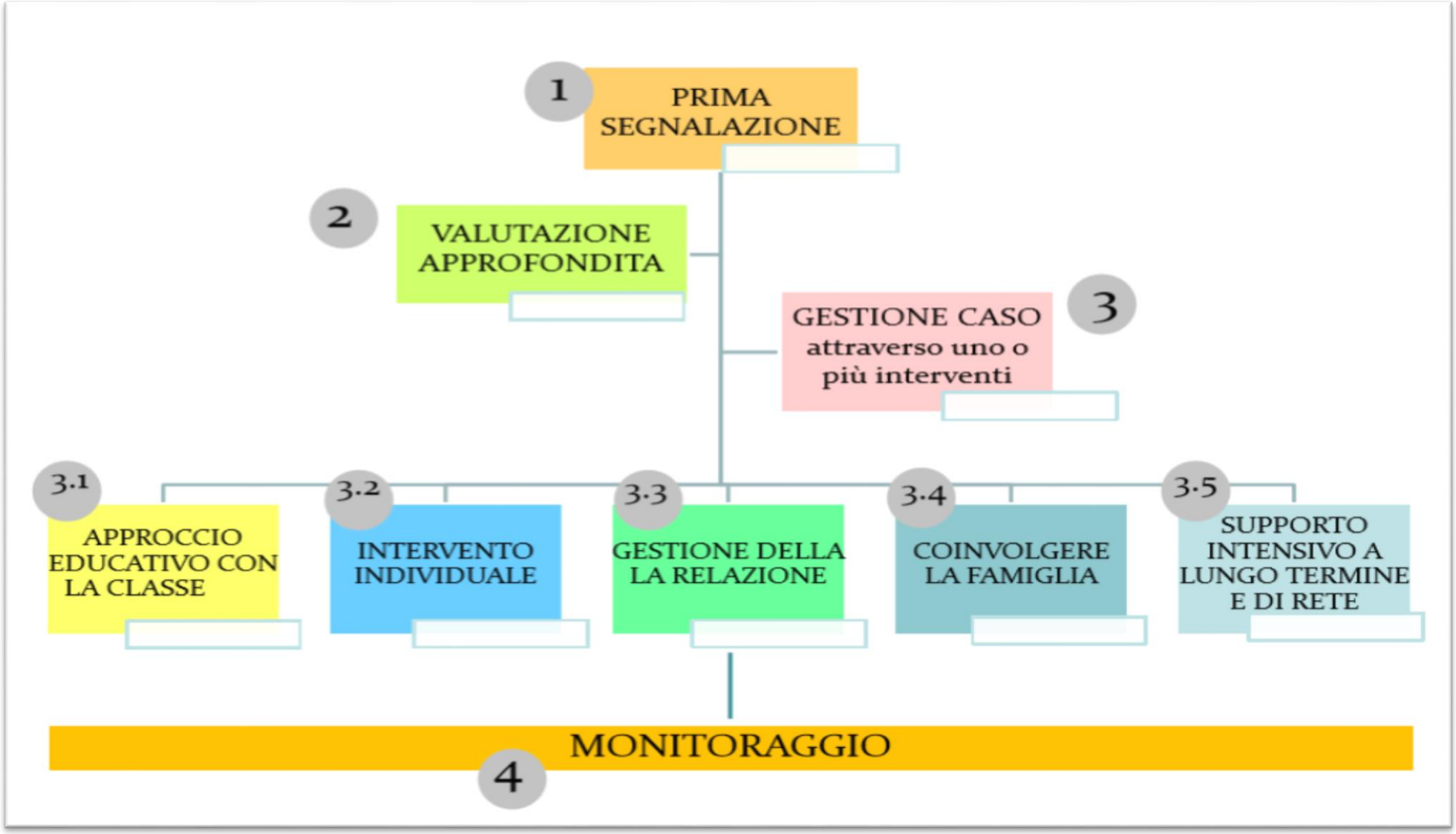
Vengono intrapresi anche i percorsi individualizzati di sostegno alle vittime, volti a incrementarne l'autostima e l'assertività e a potenziare le risorse di interazione sociale, mentre i prevaricatori sono destinatari di interventi mirati a smuoverne le competenze empatiche e a favorire una loro condivisione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

Anche in relazione alle manifestazioni socio-affettive fra pari, al linguaggio sessualizzato o "volgare", al fine di evitare prevaricazioni e imbarazzo o disagio, i docenti intervengono per favorire un buon rapporto con il proprio corpo e per far percepire meglio eventuali violazioni dei limiti di prossimità o di "confidenza" ed imparare ad opporvisi, per far acquisire fiducia nelle proprie sensazioni e nel proprio intuito e determinazione nel rifiutare i contatti anche "a distanza" sgradevoli o "strani", per rendere consapevoli gli alunni del diritto al rispetto dei propri limiti e di quelli altrui, per far capire ai ragazzi che l'interazione on-line deve sottostare a delle regole di buon comportamento, né più né meno della comunicazione a viso aperto, quale quella della vita reale.

Inoltre la scuola, qualora rilevi una situazione psico-socio-educativa particolarmente problematica, convoca i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi. Consiglia altresì di servirsi dello sportello di ascolto psicologico gratuito se attivo presso la scuola. Promuove e supporta la richiesta delle famiglie rivolta ai Servizi Sociali dell'Ente Locale per la fruizione di servizi socio-educativi comunali e alla ASL per quanto di competenza psicologica e psicoterapeutica

Scheda di segnalazione

Scheda di segnalazione in caso di presunto bullismo e vittimizzazione


1
PRIMA SEGNALAZIONE
2
VALUTAZIONE APPROFONDITA
GESTIONE CASO attraverso uno o più interventi
3
3.1
APPROCCIO EDUCATIVO CON LA CLASSE
3.2
INTERVENTO INDIVIDUALE
3.3
GESTIONE DELLA LA RELAZIONE
3.4
COINVOLGERE LA FAMIGLIA
3.5
SUPPORTO INTENSIVO A LUNGO TERMINE E DI RETE
MONITORAGGIO
4

Nel caso in cui si verifichino episodi di bullismo o di cyberbullismo e la scuola sia chiamata ad utilizzare sanzioni, saranno privilegiate azioni di supporto rispetto a provvedimenti solo punitivi, questo per non rafforzare l'identità negativa del bullo, per non amplificare il suo isolamento e indurlo alla dispersione. Nello specifico, la procedura che la scuola intende mettere in atto è la seguente:

<table>
<tr><td colspan="2">1 SEGNALAZIONE</td><td colspan="2">←Genitori
← Docenti
← Dirigente scolastico</td></tr>
<tr><td colspan="2">2a TEAM ANTIBULLISMO</td><td colspan="2" rowspan="2">←Dirigente scolastico
← Docente/i referente/i
← Rappresentanti dei genitori</td></tr>
<tr><td colspan="2">2b RACCOGLIERE DATI /VALUTARE</td></tr>
<tr><td colspan="2">3a INTERVENTI EDUCATIVI</td><td colspan="2">3b MISURE DISCIPLINARI</td></tr>
<tr><td>Soggetti coinvolti</td><td>▪ Team antibullismo
▪ Genitori
▪ Docenti
▪ Psicologo
▪ Studenti</td><td>Soggetti coinvolti</td><td>▪ Dirigente scolastico
▪ Studenti
▪ Docenti
▪ Genitori
▪ Consiglio di Classe
▪ Consiglio di Istituto</td></tr>
</table>

Interventi	Incontri con gli alunni coinvolti e colloqui con gli studenti ▪ Coinvolgimento dei genitori per informarli e predisporre strategie condivise ▪ Confronto tra i docenti ▪ Ripristino delle regole di convivenza civile all'interno della classe ▪ Lezioni dei docenti della scuola e incontri con esperti sui temi del bullismo e cyberbullismo ▪ Counselling (sportello di ascolto psicologico) ▪ Educazione tra pari (*peer education*)	Interventi /misure educative	▪ Lettera disciplinare ai genitori ▪ Lettera di scuse da parte del bullo ▪ Scuse in un incontro con la vittima ▪ Compiti /servizi di utilità sociale a favore della comunità scolastica.

4 **VALUTAZIONE EX POST**	
Se il problema è risolto: rimanere attenti. Se la situazione continua: proseguire con gli interventi.	← Genitori ←Team anti bullismo ←Studenti ← Rete del territorio (mondo accademico o mondo istituzionale).

Modello per la segnalazione di presunti casi di Bullismo cyberbullismo

(ai sensi dell'art. 2, comma 2, legge 29 maggio 2017, n. 71, Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo)

All'attenzione del Dirigente Scolastico

Referente per la prevenzione e il contrasto del bullismo e del cyberbullismo

Nome di chi compila la segnalazione_____

Data_____

Chi ha segnalato il caso di presunto bullismo-cyberbullismo era:

Studente/ssa_____

- ☐ Un compagno della vittima (nome)_____
- ☐ Madre/padre/tutore della vittima (nome)_____
- ☐ Insegnante (nome)_____
- ☐ Personale ATA (nome)_____

  Altro_____

Vittima_____Classe_____

Altra vittima_____Classe_____

Altra vittima_____Classe_____

Bullo o bulli (presunti)

Nome_____ Classe_____

Nome_____ Classe_____

Nome_____ Classe_____

SEGNALA

1. di essere stato/a vittima di cyberbullismo In particolare, i comportamenti posti in essere, **realizzati per via telematica** e di seguito sinteticamente descritti, consistono in (*selezionare la voce interessata):*
   - ☐ pressione
   - ☐ aggressione

- ☐ molestia
- ☐ ricatto
- ☐ ingiuria
- ☐ denigrazione
- ☐ diffamazione
- ☐ furto d'identità
- ☐ alterazione, acquisizione illecita, manipolazione, trattamento illecito di da
- ☐ Altro_____

  _____

2. che la diffusione di contenuti lesivi è avvenuta :

- ☐ sul sito internet _____ all'indirizzo web [ ] _____
- ☐ *social media* _____
- ☐ altro (specifica)_____

3. Allega i seguenti documenti (ad es. immagini, video, *screenshot*, etc.):

1) _____
2) _____
3) _____

4. Inserire una sintetica descrizione dei fatti:

_____
_____
_____
_____
_____

5. Quante volte si è verificato il problema_____

Il/La sottoscritto/a dichiara inoltre di

- ☐ aver presentato denuncia/querela per i fatti sopra descritti presso _____;
- ☐ non aver presentato denuncia/querela per i fatti sopra descritti.

Luogo, data

Nome e cognome

Modello per la segnalazione/reclamo in materia di cyberbullismo

(ai sensi dell'art. 2, comma 2, legge 29 maggio 2017, n. 71, Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo)

Al Garante per la protezione dei dati personali
Inviare all'indirizzo e-mail: cyberbullismo@gpdp.it

Il/La sottoscritto/a _____([1]), nato/a a _____, il _____, residente a _____, via/p.za _____, tel. _____, e-mail/PEC _____ *[inserire recapiti ai quale si può essere contattati e selezionare, di seguito, l'opzione pertinente]*,

- ☐ minore ultraquattordicenne,

ovvero

- ☐ in qualità di esercente la potestà genitoriale sul minore _____, nato a _____ il _____.

SEGNALA

6. di essere stato/a vittima ovvero che il minore sul quale esercita la potestà genitoriale è stato vittima di cyberbullismo [*eliminare la locuzione che non interessa*]. In particolare, i comportamenti posti in essere, **realizzati per via telematica** e di seguito sinteticamente descritti, consistono in [*selezionare la/e fattispecie rilevanti*]

- ☐ pressione
- ☐ aggressione
- ☐ molestia
- ☐ ricatto
- ☐ ingiuria
- ☐ denigrazione
- ☐ diffamazione
- ☐ furto d'identità
- ☐ alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati

[1] Avvertenza: la segnalazione o il reclamo può essere presentata direttamente anche da minori d'età ultraquattordicenni ovvero da chi esercita la potestà genitoriale. Pertanto si prega il segnalante/reclamante di fornire le pertinenti informazioni.

ovvero

- ☐ diffusione di contenuti *on line* aventi ad oggetto il minore ovvero uno o più componenti della famiglia del minore *[rimuovere l'informazione non rilevante]* allo scopo intenzionale e predominante di isolare il minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo.

7. che la diffusione di contenuti lesivi dell'interessato/a è avvenuta [*selezionare la casella pertinente*]:

- ☐ sul sito internet _____ all'indirizzo web [*necessario indicare URL*]
  _____
- ☐ *social media* [*necessario inserire individuazione univoca*]
  _____
- ☐ altro [*necessario specificare*]
  _____

8. Allega i seguenti documenti (ad es. immagini, video, *screenshot*, etc.):

4) _____
5) _____
6) _____

9. Inserire una sintetica descrizione dei fatti:

_____
_____
_____
_____
_____
_____

Tanto premesso, [*selezionare l'opzione pertinente*]

- considerato che il gestore del sito internet o del *social media* al quale è stata presentata l'istanza allegata per l'oscuramento, la rimozione o il blocco dei dati personali diffusi in internet non ha comunicato di

avere assunto l'incarico di provvedere all'oscuramento, alla rimozione o al blocco richiesto, né vi ha provveduto entro quarantotto ore dal ricevimento della richiesta *[allegare la pertinente documentazione]*;

- considerato che non è stato in grado di presentare un'istanza per l'oscuramento, la rimozione o il blocco dei dati personali diffusi in internet al gestore del sito internet o del *social media* non essendo possibile identificare il titolare del trattamento o il gestore del sito internet o del *social media*,

RICHIEDE AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

di disporre, ai sensi degli articoli 2, comma 2, l. n. 71/2017 nonché 143 e 144, d.lgs. n. 196/2003, il blocco/divieto della diffusione dei dati personali sopra descritti.

Il/La sottoscritto/a dichiara inoltre di *[selezionare la casella pertinente]:*

- ☐ aver presentato denuncia/querela per i fatti sopra descritti presso _____;
- ☐ non aver presentato denuncia/querela per i fatti sopra descritti.

Luogo, data

Nome e cognome

Informativa ai sensi dell'art. 13 del Codice in materia di protezione dei dati personali

Il Garante per la protezione dei dati personali tratterà i dati personali trasmessi, con modalità elettroniche e su supporti cartacei, per lo svolgimento dei compiti istituzionali nell'ambito del contrasto del fenomeno del cyberbullismo. Il loro conferimento è obbligatorio ed in assenza degli stessi la segnalazione/reclamo potrebbe non poter essere istruita. I dati personali potrebbero formare oggetto di comunicazione ai soggetti coinvolti nella trattamento dei dati personali oggetto di segnalazione/reclamo (con particolare riferimento a gestori di siti internet e social media), all'Autorità giudiziaria o alle Forze di polizia ovvero ad altri soggetti cui debbano essere comunicati per dare adempimento ad obblighi di legge. Ciascun interessato ha diritto di accedere ai dati personali a sé riferiti e di esercitare gli altri diritti previsti dall'art. 7 del Codice.

Approvato dal collegio dei docenti il 27 marzo 2019 e dal consiglio d’istituto il 28 aprile 2019