ISTITUTO COMPRENSIVO STATALE *"Pietro Carrera"*
Viale Regina Margherita, 15 - Tel. 095/7942200 - fax 095/7942210
95043 MILITELLO IN VAL DI CATANIA (CT)
C.F. 80011340876 * Cod. Mecc. CTIC835008 * E-MAIL
ctic835008@istruzione.it

IC - MILITELLO IN VAL DI CATANIA
Prot. 0000293 del 22/01/2020
01-01 (Uscita)

DOCUMENTO DI
E-SAFETY POLICY

-SICUREZZA IN RETE-

ANNO SCOLASTICO 2019/2020

1. Introduzione

1.1. Scopo della Policy

Il presente documento ha lo scopo di descrivere le norme comportamentali e le procedure per l'utilizzo delle ICT nell'Istituto Comprensivo "Pietro Carrera" di Militello in Val di Catania, le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse a un uso non consapevole delle tecnologie digitali.

La nostra Scuola intende produrre un Piano d'Azione che individua il percorso e le risorse necessarie per elaborare e implementare una Policy di ESafety, individuando due obiettivi principali:

- Adottare le misure atte a facilitare e a promuovere l'uso delle ICT nella didattica e negli ambienti scolastici;
- Stabilire le misure di prevenzione e di gestione di situazioni problematiche relative all'uso delle tecnologie digitali.

1.2. Ruoli e responsabilità (che cosa ci si aspetta da tutti gli attori della Comunità Scolastica)

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

Dirigente scolastico

- Garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- Garantire ai propri docenti una formazione di base sulle Tecnologie dell'Informazione e della Comunicazione (ICT) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse;
- Garantire l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on line.

Animatore digitale

- Formazione interna
    1. Stimolare la formazione interna alla scuola negli ambiti del PNSD, attraverso l'organizzazione di laboratori formativi, favorendo l'animazione e la partecipazione di tutta la comunità scolastica alle attività formative, come ad esempio quelle organizzate attraverso gli snodi formativi;
- Coinvolgimento della comunità scolastica
    2. Favorire la partecipazione e stimolare il protagonismo degli studenti nell'organizzazione di workshop e altre attività, anche strutturate, sui temi del PNSD, anche attraverso momenti formativi aperti alle famiglie e ad altri attori del territorio, per la realizzazione di una cultura digitale condivisa;
- Creazione di soluzioni innovative
    3. Individuare soluzioni metodologiche e tecnologiche sostenibili da diffondere all'interno degli ambienti della scuola (es. uso di particolari strumenti per la didattica di cui la scuola si è dotata; adozione di metodologie comuni; informazione su innovazioni

esistenti in altre scuole; laboratorio di coding per tutti gli studenti), coerenti con l'analisi dei fabbisogni della scuola stessa, anche in sinergia con attività di assistenza tecnica condotta da altre figure.

Direttore dei Servizi Generali e Amministrativi

- Assicurare, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione richiesti da cattivo funzionamento e/o danneggiamento della dotazione tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate;
- Facilitare la trasmissione di comunicazioni relative alle tecnologie digitali tra le varie componenti della scuola (Dirigente scolastico, Animatore digitale, docenti e famiglie degli alunni);
- Curare la registrazione dei disservizi e delle problematiche relative alla rete e all'uso del digitale segnalate dai docenti, provvedendo all'intervento del personale tecnico di assistenza.

Docenti

- Provvedere personalmente alla propria formazione/aggiornamento sull'utilizzo del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in Internet e dell'immagine degli altri: lotta al cyberbullismo);
- Sviluppare le competenze digitali degli alunni e fare così in modo che conoscano e seguano le norme di sicurezza nell'utilizzo del web e utilizzino correttamente le tecnologie digitali sia a scuola sia nelle attività didattiche extracurricolari;
- Segnalare prontamente alle famiglie eventuali problematiche emerse in classe nell'utilizzo del digitale e stabilire comuni linee di intervento educativo per affrontarle;
- Segnalare al Dirigente scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazioni.

Alunni

- Ascoltare e seguire le indicazioni fornite dai docenti per un uso corretto e responsabile delle tecnologie digitali, attuando le regole di e-safety per evitare situazioni di rischio;
- Chiedere l'intervento dell'insegnante e/o dei genitori nello svolgimento dei compiti a casa per mezzo del digitale, qualora insorgano difficoltà o dubbi nel suo utilizzo.

Genitori

- Contribuire, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- Incoraggiare l'impiego delle ICT da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza;
- Agire in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite.

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

Condivisione e comunicazione della Policy agli alunni:
All'inizio dell'anno, in occasione della illustrazione del regolamento d'istituto agli alunni da parte dei docenti, verrà presentata questa policy, insieme ai regolamenti correlati. Nel corso dell'anno saranno dedicate da ciascun docente alcune lezioni alle buone pratiche per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta al cyberbullismo.
Condivisione e comunicazione della Policy al personale:
Le norme adottate dalla scuola in materia di sicurezza nell'utilizzo del digitale saranno discusse negli organi collegiali (collegio docenti, riunioni di dipartimento, consigli di classe) e rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito web della scuola. Il personale della scuola riceverà un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso materiali resi disponibili anche sul sito web della scuola.
Condivisione e comunicazione della Policy ai genitori:
Le famiglie saranno informate in merito alla linea di condotta adottata dalla scuola per un uso sicuro e responsabile delle tecnologie digitali e di internet attraverso la condivisione del presente documento e di materiali informativi specifici sul sito web della scuola. Al fine di sensibilizzare le famiglie sui temi dell'uso delle ICT saranno organizzati dalla scuola incontri informativi, durante i quali si farà riferimento alla presente policy.

1.4. Gestione delle infrazioni alla Policy
In relazione a quanto specificato in questa policy (e in modo particolare nella definizione dei ruoli del capitolo 1.2 e nelle regole descritte nei capitoli 3, 4 e 5), le infrazioni saranno gestite in modo graduale rispetto alla gravità dell'infrazione e, nel caso degli alunni, anche alla loro età.
Infrazioni degli alunni
È 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, ogniqualvolta avvenga un'infrazione alle regole stabilite, gli strumenti per affrontare le conseguenze dei loro errori. I provvedimenti disciplinari da adottare da parte del consiglio di classe nei confronti dell'alunno che ha commesso un'infrazione alla policy (in proporzione sia all'età dello studente sia alla gravità dell'infrazione commessa) saranno i seguenti:

- Richiamo verbale;
- Sanzioni estemporanee commisurate alla gravità della violazione commessa (assegnazione di attività aggiuntive da svolgere a casa su temi di Cittadinanza e Costituzione; divieto temporaneo di prendere parte alla ricreazione e simili);
- Nota informativa sul diario ai genitori e convocazione dei genitori per un colloquio con l'insegnante;
- Convocazione dei genitori per un colloquio con il Dirigente scolastico.

Infrazioni del personale scolastico
Le infrazioni alla policy da parte del personale scolastico possono riguardare sia la mancata osservanza delle regole qui descritte sulla gestione della strumentazione, sia la mancata sorveglianza e pronto intervento nel caso di infrazione da parte degli alunni. Nel primo caso la gravità si valuta sull'esposizione al rischio procurata agli alunni, nel secondo caso sul danno per la non tempestiva attivazione delle azioni qui indicate. La gestione delle infrazioni in quest'ambito ricade nella disciplina contrattuale.
Infrazioni dei genitori

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.

1.5. Monitoraggio dell'implementazione della Policy e suo aggiornamento

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, anche attraverso la somministrazione ad alunni e docenti di questionari atti a verificare l'insorgenza di nuove necessità e la revisione di tecnologie esistenti.

1.6. Integrazione della Policy con Regolamenti esistenti

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

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

2. Formazione e Curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

In quest'ambito si seguono le indicazioni contenute nel PNSD (azione 14), in cui si individuano alcuni framework di riferimento per la definizione e lo sviluppo delle competenze digitali, tra cui il framework DIGCOMP, che prevede 21 competenze, di cui alcune specifiche nell'area della sicurezza.

2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica

Le attività di formazione si svolgeranno su due livelli:

- ❖ Formazione istituzionale, organizzata dal Miur secondo il PNSD, attraverso gli snodi formativi;
- ❖ Formazione specifica di Istituto, legata alle esigenza formative rilevate ad inizio d'anno a cura dell'Animatore Digitale, sulla base del framework DIGCOMP, come da progetto incluso nel PTOF.

2.3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

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), il nostro Istituto intende:

- ❖ Analizzare il fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica;

- Promuovere la partecipazione del corpo docente a corsi di formazione sull'utilizzo e l'integrazione delle TIC nella didattica;
- Monitorare le azioni svolte per mezzo di un questionario di autovalutazione;
- Organizzare incontri con esperti.

2.4. Sensibilizzazione delle famiglie

Il nostro Istituto, pertanto, organizzerà incontri aperti alle famiglie e agli studenti con enti esterni, come la Polizia Postale, per sensibilizzare docenti, alunni e genitori sui temi della sicurezza online, per offrire occasioni di confronto e discussione sui rischi rappresentati dall'uso di smartphone e chat line senza un'adeguata formazione in merito ai rischi derivanti da un uso inappropriato di tali dispositivi. La Scuola darà, inoltre, ampia diffusione, tramite pubblicazione sul sito, del presente documento di policy per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e favorire un'attiva collaborazione tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi a un uso inappropriato del digitale.

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

3.1. Accesso a internet: filtri, antivirus e sulla navigazione

L'accesso a internet è possibile, nei due plessi della scuola e in tutte le aule, dotate di Lavagna Interattiva Multimediale con relativo computer portatile custodito in un cassetto chiuso a chiave. Inoltre, l'accesso a internet è possibile anche dal laboratorio di informatica e da un ambiente con postazioni PC a disposizione del personale. Nei laboratori di informatica e nelle aule sono attivi filtri per la navigazione sicura, tramite gestione di blacklist, ed è prevista l'attivazione di software per la gestione e il controllo delle postazioni. Le impostazioni sono definite e manutenute 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.

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

Nei computer presenti nelle aule e nei laboratori sono previsti tre profili di accesso con password relative: amministratore; docente; alunno. È possibile effettuare installazioni e aggiornamenti di software solo tramite la password di amministratore, fornita al personale di assistenza tecnica e all'Animatore Digitale. Non è previsto un backup automatico su server e non è al momento attiva una politica di backup.

3.3. E-mail

L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. Le credenziali sono in possesso del personale amministrativo. I docenti utilizzano per scopi didattici il proprio account su dominio istruzione.it. La posta elettronica è protetta da antivirus e da antispam.

3.4. Blog e sito web della scuola

La scuola ha un sito web e in alcune classi è utilizzato un wiki. Tutti i contenuti del settore didattico sono pubblicati direttamente sotto supervisione dell'Animatore digitale, che ne valuta con il Dirigente scolastico la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc. Per il wiki o altri siti web di classe o di progetto, le regole di utilizzo sono definite dall'Animatore Digitale e applicate dai docenti di classe.

3.5. Social network.
Attualmente nella didattica non si utilizzano social network, neanche da parte dell'istituzione scolastica, e il personale scolastico non è autorizzato a utilizzarli per nome e per conto della stessa.

3.6. 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 su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi. Viene, inoltre, fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori.

4. Strumentazione personale

4.1. Per gli studenti: gestione degli strumenti personali – cellulari, tablet, ecc.
Come espresso nel Patto di corresponsabilità, gli alunni si impegnano a tenere spenti i telefoni cellulari e a consegnarli al docente all'ingresso in classe. In caso di urgenza per comunicazioni tra gli alunni e le famiglie, su autorizzazione dei docenti e sotto il diretto controllo dei collaboratori scolastici, gli alunni potranno comunicare con le famiglie tramite gli apparecchi telefonici della scuola. Non è consentito l'uso di dispositivi personali.

4.2. Per i docenti: gestione degli strumenti personali – cellulari, tablet, ecc.
Durante le ore di lezione è consentito ai docenti l'uso di dispositivi elettronici personali, come il tablet, unicamente a scopo didattico e a integrazione dei dispositivi scolastici disponibili (il computer di classe), in special modo per l'utilizzo del registro elettronico. Durante il restante orario di servizio l'uso del cellulare è consentito solo per comunicazioni personali che rivestano carattere di urgenza, mentre l'uso di altri dispositivi elettronici personali è permesso per attività funzionali all'insegnamento.

4.3. Per il personale della scuola: gestione degli strumenti personali – cellulari, tablet, ecc.
Durante l'orario di servizio al restante personale scolastico l'uso del cellulare è consentito per comunicazioni personali urgenti. L'uso di altri dispositivi elettronici personali è permesso solo per attività funzionali al servizio, e preventivamente autorizzato.

5. Prevenzione, rilevazione e gestione dei casi

5.1. Prevenzione

5.1.1. Rischi

La prima responsabilità degli insegnanti consiste nell'imparare a riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente. Tra questi, un'attenzione specifica andrà prestata ai fenomeni di: bullismo/cyberbullismo – una forma di prepotenza virtuale attuata attraverso l'uso di internet e delle tecnologie digitali; sexting - pratica di inviare o postare messaggi di testo e immagini a sfondo sessuale, come foto di nudo o semi-nudo, via cellulare o tramite Internet (Levick& Moon 2010) – e adescamento o grooming – una tecnica di manipolazione psicologica, che gli adulti potenziali abusanti utilizzano online, per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata (Glossario di "Generazioni connesse"). I rischi che i ragazzi possono correre a scuola nell'utilizzo di dispositivi digitali possono derivare principalmente da un uso non corretto del telefono cellulare o di altri dispositivi come lo smartphone o il tablet. Sebbene, infatti, l'uso del

cellulare e dello smartphone non sia consentito dal Regolamento dell'Istituto, molti bambini della scuola primaria e quasi tutti i ragazzi della secondaria vengono a scuola con uno di questi dispositivi che dovrebbero tenere spenti durante le lezioni. Accade purtroppo, che in orario scolastico, alcuni studenti, eludendo la sorveglianza del personale della scuola, accendano e adoperino il cellulare o lo smartphone, non solo per comunicare con i propri genitori, ma anche per navigare su internet, andando su siti non adatti e inviando materiali riservati (foto, video e altro). Così facendo, gli studenti possono incorrere anche a scuola nei rischi che abbiamo menzionato sopra, entrando in contatto e persino in confidenza con sconosciuti, fino a ricevere messaggi molesti e adescamenti.

5.1.2. Azioni

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

- Diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web, condividendo materiali messi a disposizione sul sito del progetto "Generazioni connesse";
- Richiedere di volta in volta autorizzazione esplicita da parte dei genitori all'utilizzo dei dati personali degli alunni (es. liberatoria per la pubblicazione di foto, immagini, video relativi al proprio/a figlio/a per la partecipazione a progetti didattici e altro);
- Far rispettare il divieto di utilizzo di dispositivi digitali propri, quali cellulare e smartphone, agli studenti in orario scolastico. Le dovute eccezioni (uso del cellulare per comunicazioni alunno-famiglia in occasione di uscite didattiche) andranno espressamente regolamentate e dovranno comunque avvenire sotto la supervisione diretta di un docente responsabile;
- Dotare i dispositivi della scuola di filtri che impediscano l'accesso a siti web non adatti ai minori (black list).

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

- Bloccare l'accesso a un sito o a un insieme di pagine impedendone la consultazione;
- Controllare periodicamente i siti visitati dagli alunni;
- Utilizzare un software in grado di intercettare le richieste di collegamento e di respingere quelle non conformi alle regole stabilite dall'amministratore;
- Affidare a un gruppo di docenti scelto le regole di filtraggio.

5.2. Rilevazione

5.2.1. Che cosa segnalare

Tra i contenuti devono essere opportunamente segnalati:

- Dati sensibili o riservati (foto, immagini, video personali, informazioni private proprie o di amici; l'indirizzo di casa o il telefono, ecc.);
- Contenuti che possano considerarsi in qualche modo lesivi dell'immagine altrui (commenti offensivi, minacce, osservazioni diffamatorie o discriminatorie, foto o video denigratori, videogiochi che contengano un'istigazione alla violenza, ecc.);

- Contenuti riconducibili alla sfera sessuale: messaggi, immagini o video a sfondo sessuale, come foto di nudo o semi-nudo, ecc.

5.2.2. Come segnalare: quali strumenti e a chi

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

- A una comunicazione scritta tramite diario alle famiglie;
- A una nota disciplinare sul Diario di classe;
- A una convocazione formale dei genitori degli alunni, tramite segreteria;
- A una convocazione delle famiglie da parte del Dirigente scolastico.

Per i reati più gravi la scuola si rivolgerà direttamente agli organi di polizia competenti.

5.3. Gestione dei casi

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

a) Casi di cyberbullismo:

Si definiscono bullismo tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o a volte un piccolo gruppo). Si tratta, pertanto, di una serie di comportamenti portati avanti ripetutamente nel tempo. Si parla di cyberbullismo quando queste forme di prevaricazione reiterate nel tempo si estendono anche alla vita online. Tale specifica forma di bullismo ha caratteristiche peculiari:
1) è pervasivo, il bullo può raggiungere la sua vittima in qualsiasi momento e in qualunque luogo;
2) è un fenomeno persistente: il materiale messo online vi può rimanere per molto tempo;
3) spettatori e cyberbulli sono potenzialmente infiniti, le persone che possono assistere agli atti di cyberbullismo sono potenzialmente illimitate.
Occorre tenere presente che il cyberbullo non è mai del tutto consapevole della gravità dei suoi comportamenti se non viene aiutato ad esserne consapevole.

Qualora ci si trovi di fronte ad un caso di cyberbullismo si dovrà:

- Informare i genitori degli alunni coinvolti;
- Coinvolgere il referente di istituto dell'e-safety e gli operatori scolastici su quanto sta accadendo;

- Coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online;
- Tenere traccia di quanto successo e delle azioni intraprese, compilando un "diario di bordo" per consentire ulteriori indagini se necessarie.

b) Casi di sexting:

Qualora ci si trovi di fronte a un caso di sexting (con cui si intende l'invio e/o la ricezione e/o la condivisione di testi, video o immagini sessualmente esplicite via cellulare o tramite internet) si dovrà:

- Coinvolgere la classe e confrontarsi con esperti, facendo appello, per esempio, allo sportello d'ascolto dell'istituto per capire come approfondire e affrontare il fenomeno;
- Coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti riconducibili al sexting;
- Documentarsi opportunamente sulle norme giuridiche che regolano i comportamenti e le condotte sessuali in Italia;
- Intraprendere con la classe attività mirate a riflettere sulla fiducia che ciascuno ripone negli altri e sul fenomeno del sexting, approfondendo casi e testimonianze.

c) Casi di adescamento online o grooming:

L'adescamento online (grooming) consiste nel tentativo, da parte di un adulto, di avvicinare un/a bambino/a o adolescente per scopi sessuali, conquistandone la fiducia attraverso l'utilizzo della rete Internet (tramite chat, blog, forum e social networks, per esempio). È bene che anche gli insegnanti aiutino i propri alunni a tutelarsi, scegliendo con cura chi frequentare online, per evitare che una condotta imprudente possa comportare ripercussioni non banali nella loro vita reale. Una volta riconosciuti alcuni segni che possono rinviare a una situazione di adescamento online, quali un improvviso calo nel rendimento scolastico, un aumento del tempo trascorso dall'alunno online congiunto ad una particolare riservatezza al riguardo, allusioni da parte dell'alunno alla frequentazione di una persona più grande, o a regali ricevuti, ecc., è bene:

- Approfondire la situazione coinvolgendo la classe e l'intera comunità scolastica;
- Avviare dei percorsi di riflessione in classe sul concetto di fiducia;
- Farsi affiancare da esperti, ricorrendo anche allo sportello d'ascolto per offrire ai minori, qualora lo desiderino, il supporto necessario.

Le procedure, da applicarsi secondo i criteri dettati dalla policy, sono incluse nel Codice Disciplinare, nel Patto di corresponsabilità e nel PTOF. Le procedure operative per la protezione dei dati personali sono incluse nel Regolamento d'istituto, parte integrante del PTOF. Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni sono incluse nel Patto di corresponsabilità.

Militello in Val di Catania, 19 Dicembre 2019

Il Referente del Bullismo/Cyberbullismo

Prof.ssa Maria Gabriella Cannizzaro

ISTITUTO COMPRENSIVO STATALE "GIOVANNI VERGA" SCORDIA (CT)

Il Dirigente Scolastico

Prof. Giuseppe Calleri

Nome: Utente
Motivo: Conformato
Data: 22/01/2020 12:23:28 (UTC+01:00)