ISTITUTO COMPRENSIVO DI SCUOLA DELL´INFANZIA, PRIMARIA E SECONDARIA DI PRIMO GRADO
"B. CROCE " - 65020 SAN VALENTINO IN A.C. (PE) VIA LARGO S. NICOLA
Tel. : 085/8574134 – Fax 085/8577825 - COD. FISC.: 81002100683
E mail – peic81000v@istruzione.it - peic81000v@pec.istruzione.it
www.icsanvalentino.gov.it

A.S. 2018/2019

POLICY e-SAFETY

Generazioni Connesse
SAFER INTERNET CENTRE

Policy e - Safety

INDICE DEI CONTENUTI

1. Introduzione

1.1 Scopo, definizione e destinatari della Policy

La tecnologia e Internet hanno repentinamente rivoluzionato il modo di vivere della nostra società, facilitando l'accesso alle informazioni, il modo di comunicare, di esprimere e di condividere conoscenze, pensieri e stati d'animo, e di svolgere operazioni e servizi quotidiani e tradizionali.

Se, da un lato, in ambito scolastico, la diffusione delle tecnologie digitali ha offerto nuove opportunità ed apportato cambiamenti ai tempi e alle modalità dell'insegnamento e dell'apprendimento, è anche vero che, dall'altro, il facile accesso alle tecnologie delle informazioni e delle comunicazioni deve far riflettere le istituzioni scolastiche sull'uso corretto e consapevole e sui rischi ai quali i ragazzi, i "nativi digitali, sono spesso esposti, imbattendosi, spesso inconsapevolmente, in situazioni rischiose e problematiche.

Per il suo ruolo educativo, la scuola è pertanto chiamata ad elaborare una politica di sicurezza della navigazione *on line* volta ad un controllo dell'uso delle strumentazioni digitali e alla diffusione dell'adozione di buone pratiche di navigazione su *Internet.*

Al fine di promuovere un uso sicuro e positivo delle tecnologie tra gli studenti, il nostro Istituto ha aderito al progetto SIC (Safer Internet Centre) - "Generazioni Connesse", promosso dal Miur, nell'ambito del quale ha elaborato il presente documento di **Policy e-Safer**. In esso si delineano i principi fondamentali, le norme comportamentali e le procedure per utilizzare correttamente le TIC e le risorse informatiche di cui il nostro Istituto è dotato.

Con la presente *Policy* si vogliono altresì definire le misure di prevenzione, rilevazione e gestione delle problematiche connesse all'uso improprio della strumentazione digitale anche attraverso la formazione degli insegnanti e la sensibilizzazione dei genitori, allo scopo di attuare attività di prevenzione, controllo e riduzione di azioni che possono rivelarsi spiacevoli per la comunità scolastica o addirittura configurarsi come reati.

La presente *Policy* si rivolge:

- agli alunni della Scuola Primaria;
- agli alunni del triennio della Secondaria di primo grado;
- ai docenti che svolgono la loro attività di insegnamento nei tre ordini di scuola del nostro Istituto, sia a tempo indeterminato che determinato;
- al Dirigente Scolastico e al Dirigente dei Servizi Amministrativi;
- agli operatori esterni che entrano in relazione con i nostril studenti in qualità di assistente educativo, esperti di progetto, assistenti di mensa, ecc.
- ai genitori tutti
- ai visitatori/ospiti.

Il documento potrà essere modificato e aggiornato annualmente 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.

1.2 Ruoli e responsabilità

Il Dirigente Scolastico:

- deve tutelare la scuola e promuovere tutte le procedure di sicurezza (tra cui la sicurezza on line) dei membri della comunità scolastica;
- ha la responsabilità della gestione dei dati e della sicurezza delle informazioni e garantisce che l'Istituto segua le migliori pratiche possibili nella gestione dei dati stessi;
- deve garantire che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della Comunicazione (TIC);
- deve garantire agli utenti la sicurezza di navigazione utilizzando adeguati sistemi informatici e servizi di filtri Internet;
- coerentemente con l'analisi dei fabbisogni della scuola, promuove la partecipazione alle attività formative della comunità scolastica globalmente intesa, a partire dagli studenti, anche attraverso momenti informativi e di sensibilizzazione aperti alle famiglie e ad altri attori del territorio;
- deve garantire adeguate valutazioni di rischio nell'usare strumenti e TIC, in modo che quanto programmato possa soddisfare le istanze educative e didattiche dichiarate nel PTOF di Istituto.

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, le famiglie e gli Enti territoriali.

L'Animatore Digitale (in collaborazione con il gruppo di lavoro costituto dai docenti del Team dell'Innovazione e del NIV e con la Funzione Strumentale della Progettualità) collabora alla redazione e alle eventuali revisioni della *Policy* sulla base delle osservazioni ricevute da tutti i soggetti interessati, assicurando la massima diffusione del documento presso la comunità scolastica mediante pubblicazione sul sito della scuola. L'Animatore inoltre, come da Piano Nazionale Scuola Digitale (PNSD), agisce nell'ambito di

- strumenti e infrastrutture;
- contenuti e competenze;
- formazione e accompagnamento

Le figure componenti il suddetto Gruppo di lavoro sono rappresentative dei tre ordini (Infanzia Primaria e Secondaria di I grado) e dei tre plessi scolastici. Esse si fanno carico della responsabilità dei problemi di sicurezza online e sono docenti di riferimento per la creazione e la revisione delle politiche di sicurezza online della scuola e dei relativi documenti (tra cui la revisione annuale della *Policy* sulla base delle osservazioni ricevute dai

soggetti interessati). Si impegnano, inoltre, a promuovere la cultura della sicurezza on-line in tutta la comunità scolastica e devono garantire che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente di sicurezza on-line.

I Docenti devono avere adeguata consapevolezza delle questioni di sicurezza informatica, con particolare riferimento alla dimensione etica del digitale, vale a dire alla tutela della *privacy* e dell'immagine degli altri, alla prevenzione e al contrasto di fenomeni di *cyber*-bullismo. In particolare, I docenti:

- devono informarsi ed aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di Internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- devono garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di Internet;
- si devono 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;
- devono garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- devono assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllano l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
- affrontano le problematiche connesse a tali questioni tendendo a favorire, da parte degli alunni, lo sviluppo di competenze digitali, la conoscenza e il rispetto delle norme di sicurezza per un corretto utilizzo del *web* e delle tecnologie digitali, sia in ambiente scolastico, sia nelle attività extrascolastiche;
- segnalano alle famiglie eventuali problemi emersi nell'attività scolastica in merito all'uso del digitale, individuando in collaborazione con esse linee comuni di intervento educativo per affrontare tali problemi;
- supervisionano e guidano gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono tecnologie online.
- garantiscono che gli alunni siano capaci di ricercare contenuti online in sicurezza e siano pienamente consapevoli dei problemi relativi ai contenuti elettronici (come ad esempio le leggi sul copyright);
- segnalano per tempo al Dirigente Scolastico e ai suoi collaboratori eventuali violazioni delle norme di comportamento stabilite.

Il **Personale ATA** deve avere adeguata consapevolezza delle questioni di sicurezza informatica e delle relative buone pratiche adottate dall'Istituto e deve segnalare ai Docenti, al Dirigente Scolastico o ai suoi collaboratori eventuali abusi da parte degli alunni.

Gli **Alunni** sono responsabili di un corretto utilizzo dei dispositivi informatici e delle tecnologie digitali. Essi sono tenuti a:

- non utilizzare dispositivi personali durante l'attività didattica, quando non dichiaratamente consentito dai docenti;
- conoscere l'importanza dell'adozione di buone pratiche di sicurezza informatica in ogni momento della vita, allo scopo di tutelare sé stessi e gli altri, evitando di compiere atti punibili a livello scolastico e veri e propri reati;
- comprendere l'importanza di segnalare eventuali abusi, usi impropri o accessi a materiali inappropriati;
- essere consapevoli dell'importanza di un corretto utilizzo delle immagini;
- essere consapevoli del significato e della gravità del fenomeni di *cyber*-bullismo.

Genitori e famigliari svolgono un ruolo fondamentale nel guidare bambini e ragazzi verso una crescente consapevolezza nel corretto utilizzo di Internet e dei dispositivi mobili. La scuola continuerà a sensibilizzare e informare le famiglie in questo senso, attraverso incontri ed eventi aperti anche ad esse, in un'ottica di partecipazione condivisa e di inclusione.
I genitori sostengono la scuola nel promuovere la sicurezza online e approvano un accordo sull'uso accettabile delle tecnologie, che può comprendere anche l'uso concordato di device personali, di Internet attraverso la rete di Istituto e l'uso da parte della scuola di immagini fotografiche e video ai fini di documentazione didattica di eventi scolastici e partecipazione a progetti o concorsi promossi da Enti di affermata reputazione in ambito educativo o territoriale.

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

Per garantire una completa condivisione della Policy da parte dell'intera comunità scolastica e far sì che da tale documento si intraprendano successive azioni sui contenuti e sulle pratiche da adottare ed iniziative di confronto sulla eventuale necessità di apportarvi modifiche e/o integrazioni, la Policy sarà condivisa ed approvata dal Collegio dei docenti (ai quali sarà preventivamente inviate tramite mail) e dal Consiglio di Istituto e, successivamente, pubblicata sul sito web della scuola ed integrata nel PTOF.
Al nuovo personale e ai nuovi alunni sarà consegnato un estratto della Policy insieme a tutti i documenti da sottoscrivere all'atto della stipula del contratto o dell'iscrizione.

1.4 Gestione delle infrazioni alla *Policy*

Qualsiasi sospetto, rischio, violazione delle norme circa l'uso improprio può essere rilevato da docenti e dal personale ATA e va segnalato al Dirigente Scolastico che, a seconda della gravità, potrà riferire direttamente alle autorità di competenza.

I provvedimenti disciplinari nei confronti dell'alunno che ha commesso un'infrazione alla Policy saranno gestiti in relazione alla loro gravità e, nel caso degli alunni, anche alla loro età e potranno essere così graduati:

- richiamo verbale;
- sanzioni commisurate alla gravità della violazione commessa (assegnazione di attività da svolgere a casa su temi di Cittadinanza e Costituzione; divieto temporaneo di prendere parte a uscite didattiche, viaggio d'istruzione e simili);
- annotazione disciplinare sul diario al fine di informare i genitori;
- convocazione dei genitori per un colloquio con l'insegnante;
- convocazione dei genitori per un colloquio con il Dirigente scolastico.

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

Il monitoraggio per l'implementazione della Policy sarà effettuato annualmente (al termine dell'anno scolastico, contestualmente al Rapporto di Autovalutazione e sulla base dei casi problematici riscontrati e della loro gestione, oppure all'inizio dell'anno scolastico, in fase di revisione del PTOF), o qualora si verificassero cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola.

.

1.6 Integrazione della *Policy* con Regolamenti esistenti

La *Policy* è coerente con quanto è previsto e stabilito dal vigente Regolamento di Istituto e dal Patto di Corresponsabilità. Potrà essere integrata con il PTOF.

2. Formazione e curricolo

2.1 Curricolo sulle competenze digitali per gli studenti

Secondo le *Nuove Indicazioni Nazionali del 2012*, in raccordo con il *Programma Europeo per le Competenze chiave* in un mondo in trasformazione, al traguardo del Primo Grado di Istruzione lo studente dovrebbe possedere buone competenze digitali e saper usare consapevolmente le tecnologie della comunicazione per ricercare, analizzando informazioni e dati che possano aiutarlo a distinguere quelli attendibili da quelli che necessitano di approfondimento, di controllo e di verifica.

Le TIC preparano gli studenti ad un'attiva e consapevole partecipazione ad un mondo in continua evoluzione e nel quale è necessario acquisire abilità e competenze in grado di facilitare l'adattamento dell'individuo ai rapidi cambiamenti. Alla Scuola spetta il dovere di fornire loro tali strumenti informatici e di far acquisire e maturare le competenze digitali di ciascuno.

A tal fine, da diversi anni, il nostro Istituto promuove attività ed incontri di Cittadinanza digitale (anche con il supporto della Polizia Postale) rivolte soprattutto agli alunni della scuola secondaria di primo grado (soprattutto classe terza), relative all'uso corretto e consapevole degli strumenti informatici, e ai vantaggi e ai rischi di Internet.

Le attività hanno affrontato i seguenti temi:

- C**omportamento *online*** (*Social network*, *Cyber*-bullismo, *e-shopping*, sessualità in rete, *netiquette*);
- **Sicurezza su Internet** (*Phishing* e furti d'identità**,** *cookies* e *pharming*, *password* e *privacy online*, virus e *spam*)
- **Partecipazione alla campagna itinerante "Una vita da social"**;
- attività di **C*oding*** in alcune classi della scuola primaria e nella classe terza della scuola secondaria, relativamente allo sviluppo del pensiero computazionale.

Inoltre, per diversi anni, l'Istituto ha attivato corsi extrascolastici di "Eipass Junior" rivolti agli studenti della classe terza della scuola secondaria e, dal corrente anno scolastico, diverrà Centro Formatore per il conseguimento della certificazione informatica della Patente Europea.

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

Per ciò che concerne la formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica e sui temi dell'infomatica, essa può avvenire a livello interno (formazione in servizio obbligatoria ai sensi della L.107/2015) ed esterno, a discrezione e scelta del singolo insegnante tra le varie proposte di corsi, convegni e seminari riguardanti tal argomenti, la cui informzione è assicurata in maniera tempestiva dalla scuola stessa.

Nel corso degli ultimi anni scolastici, la formazione interna dei docenti sulle competenze digitali è stata imperniata sull'**utilizzo della LIM (**stili e ambienti di apprendimento integrati con la LIM; la LIM e la didattica: indicazioni operative). La Scuola può aderire a progetti appositi di formazione presentati da Enti e Associazioni.Nel precedente anno scolastico, diversi docenti appartenenti ai tre gradi d'istruzione dell'Istituto hanno partecipato ai corsi pomeridiani organizzati nell'ambito del Programma Operativo Nazionale "Per la scuola - competenze e ambienti di apprendimento" per l'acquisizione delle competenze infomatiche. Gestione dell'infrastruttura e della strumentazione ICT della scuola

2.3 Accesso ad internet: filtri, antivirus e navigazione

L'Istituto ha adottato le misure minime di sicurezza.

Ogni classe dell'Istituto è dotata di PC con il quale si può accedere al Registro Elettronico in uso attraverso la rete WIFI, mentre i PC presenti nei laboratori dell'Istituto accedono attraverso la rete LAN. Tutti i dispositivi sono protetti con antivirus e software che

rimuovono automaticamente eventuali installazioni non autorizzate

2.4 Gestione accessi (*password*, *backup*, ecc.)

Ogni docente accede al Registro Elettronico attraverso una *password* personale che non può essere comunicata a terzi, né agli alunni.

2.5 Protezione dei dati personali

In merito alla protezione dei dati personali, si fa riferimento a quanto previsto dal Decreto legislative 30 Giugno 2003, n. 196 (cosiddetto Codice della *Privacy*), nonché alla recente Guida *La scuola a prova di privacy,* a cura del Garante per la Protezione dei Dati personali.

3. Strumentazione personale

3.1 Strumentazione personale nella comunità scolastica

Gli alunni possono accedere alla Rete attraverso i dispositivi della scuola e utilizzare i propri dispositivi durante le attività didattiche solo se autorizzati dai docenti presenti in aula e esclusivamente per finalità attinenti alle attività didattiche.

L'utilizzo a scuola dei propri device (BYOD Bring Your Own Device) è da considerarsi un'opportunità didattica ed andrà concordato con genitori dagli insegnanti che useranno tali strumenti in classe. Ogni altro uso è vietato.

Il divieto si applica all'orario delle lezioni e vale anche negli intervalli e nelle altre pause dell'attività didattica e negli altri momenti di permanenza a scuola (intervallo, mensa, cambio dell'ora, ecc.).

I docenti possono utilizzare in classe i dispositivi della scuola e quelli personali per realizzare tutte le attività connesse alla funzione docente e all'attività didattica.

Il personale docente, gli studenti e tutti gli esterni che portano nell'Istituto i device di loro proprietà sono responsabili del proprio dispositivo: di eventuali danneggiamenti, furti o smarrimenti degli stessi, la scuola non potrà essere considerata responsabile.

3.2 Gestione della strumentazione personale

Ad eccezione di casi speciali e comunque sempre concordati con il corpo docente che ne delibera il modo di utilizzo, la scuola invita tutti gli studenti a non portare telefoni cellulari e dispositivi mobile personali a scuola. Per la scuola dell'infanzia il divieto è categorico.

Si ribadisce che le riprese fotografiche, vocali o video potranno essere eseguite solo per scopi didattici dichiarati, con il consenso delle parti interessate (obbligatoria liberatoria dei genitori o tutori), e tenendo conto delle recenti indicazioni del Garante della privacy .

Registrazioni o immagini effettuate durante lezioni, uscite didattiche o attività di presentazione allargate (come manifestazioni, eventi culturali ecc.) possono essere utilizzate per usi esclusivamente didattici, di divulgazione delle attività dell'Istituto e di documentazione pedagogica.

La diffusione di contenuti (che avviene attraverso canali ufficiali di proprietà della nostra scuola), è sempre subordinata all'autorizzazione del Dirigente Scolastico e al consenso da parte delle persone ritratte o riprese.

Se uno studente viola questa Policy, il dispositivo verrà in tutti i casi sequestrato e custodito in un luogo sicuro dell'edificio scolastico. I dispositivi mobili saranno rilasciati solo ai genitori o tutore con delega.

4. Prevenzione, rilevazione e gestione dei casi

4.1 Indicazioni di massima per la prevenzione dei casi

La scuola continuerà a promuovere con l'ausilio di progetti e con la collaborazione di operatori esterni campagne di sensibilizzazione e incontri informativi rivolti sia agli alunni che alle famiglie con l'intento di contribuire alla prevenzione e alla gestione delle problematiche relative alla sicurezza in rete. In particolare, da un lato, nell'ambito dell'offerta formativa che caratterizza il nostro Istituto, un' attenzione specifica è rivolta a quelle attività curricolari che promuovono approfondimenti tematici legati all'educazione all'affettività, alla legalità, alla sicurezza informatica, alla salute, alla genitorialità; dall'altro, nell'ottica di una comune azione educative, le famiglie sono invitate ad attivare forme di controllo parentale nella navigazione, a monitorare l'esperienza online dei propri figli, a partecipare agli incontri informativi organizzati o proposti dalla scuola sulla sicurezza in rete e a proporre tematiche di particolare interesse su cui l'Istituto potrà eventualmente calibrare le proprie azioni.

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

Tra questi, un'attenzione specifica andrà prestata ai fenomeni di **bullismo/cyberbullismo** (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) e **adescamento** o **grooming** (una tecnica di manipolazione psicologica, che gli adulti potenziali abusanti utilizzano online, per indurre bambini e adolescenti a superare le resistenze emotive e instaurare una relazione intima e sessualizzata).

Purtroppo, a causa di un uso non corretto dei dispositivi o smartphone, eludendo la sorveglianza, anche in orario scolastico i ragazzi possono incorrere in tali rischi.

4.2 La rilevazione dei casi

La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti e potranno avvenire mediante **osservazione** sistematica da parte dei docenti nelle classi, **richieste specifiche** ai ragazzi sul

loro benessere all'interno e all'esterno della scuola anche non necessariamente in situazione di palese disagio e ascolto attento di quanto eventualmente raccontano, **punto di raccolta segnalazioni di disagio da parte degli alunni** attraverso l'utilizzo di una cassetta in cui inserire delle comunicazioni rivolte ai docenti; essa deve essere posta in un luogo accessibile e controllato da parte del personale ausiliario. Tale segnalazione non deve assolutamente essere scritta in forma anonima quindi deve contenente nome, cognome, classe, data ed una breve descrizione del fatto che causa disagio.

Andranno opportunamente segnalati per gli interventi opportuni i seguenti casi:

- Pubblicazione e/o diffusione di dati sensibili o riservati (foto, immagini, video personali, informazioni private proprie o altrui; l'indirizzo di casa o il numero di telefono, ecc.);
- Pubblicazione e/o diffusione di 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.);
- Pubblicazione e/o diffusione di contenuti riconducibili alla sfera sessuale: messaggi, immagini o video a sfondo sessuale, come foto di nudo o semi-nudo, ecc.

Il personale della scuola provvederà a conservare le eventuali tracce di una navigazione non consentita su internet o del passaggio di materiali inidonei sui pc della scuola nonché la data e l'ora. Nel caso di messaggi, si cercherà di risalire al mittente attraverso i dati del suo profilo. L'insegnante dovrà copiare e stampare i messaggi per fornire le eventuali prove all'indagine sugli abusi commessi e raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico, alla famiglia ed, eventualmente, alla Polizia Postale. Qualora siano coinvolti più alunni, in qualità di vittime o di responsabili della condotta scorretta, le famiglie degli alunni in questione saranno convocate e informate tempestivamente per un confronto.

Come intervenire:

- segnalazione del caso al Coordinatore della classe e al Consiglio di classe;
- parlare, ascoltare famigliari, insegnanti, amici, servizi del territorio, operatori;
- pianificare adeguati interventi educativi sia a sostegno delle vittime che nei confronti di quegli alunni che abbiano messo in atto comportamenti lesivi, coinvolgendo le rispettive famiglie in un percorso comune e condiviso di sostegno al disagio;
- nei casi di maggiore gravità si valuterà anche il coinvolgimento di attori esterni quali le Forze

dell'ordine e i servizi sociali.

In base alla gravità dei fatti si provvederà:

- a un richiamo verbale;
- a una comunicazione scritta tramite diario alle famiglie;
- a una annotazione disciplinare sul registro on-line;
- 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.

4.3 La gestione dei casi

Per tutti i casi che costituiscono reato occorre informare il Dirigente Scolastico per confrontarsi sulle azioni da intraprendere ed eventualmente attivare l'intervento delle Forze dell'ordine. Non esistono protocolli siglati con le Forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi, tuttavia si praticano forme di collaborazione nella prevenzione e contrasto del bullismo e del cyberbullismo con gli Enti locali, la Polizia Postale e il Comando dei Carabinieri.
La gestione dei casi rilevati andrà differenziata a seconda della loro gravità e sarà discussa e condivisa nel Consiglio di Classe.

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

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:

- promuovere campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni;
- 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 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, 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;
- Segnalare agli alunni l'esistenza di una linea di ascolto 19696 "Pronto Telefono Azzurro" o "Ci@o, sono Telefono Azzurro" attiva tutto l'anno 24 ore su 24 di Telefono Azzurro che raccoglie richieste di ascolto e di aiuto. Attraverso il Form di segnalazione "Clicca e Segnala" si possono segnalare contenuti illeciti (materiale pedopornografico) o potenzialmente dannosi dannosi per bambini e adolescenti.

RISCHI	AZIONI

Adescamento online (grooming)	Sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione. Qualora si venga a conoscenza di casi simili, occorre valutarne la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.
Cyberbullismo	Campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni. I casi possono essere molto variegati, variando dal semplice scherzo di cattivo gusto via sms/Whatsapp a vere e proprie minacce verbali e fisiche, che costituiscono reato. Occorre confrontarsi con il Dirigente Scolastico sulle azioni da intraprendere.
Dipendenza da Internet videogiochi, shopping o gambling online	Informazioni sul fatto che ciò può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito a insaputa di altri) rappresenta un vero e proprio illecito.

Esposizione a contenuti pornografici, violenti, razzisti	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione e sensibilizzazione sulla necessità di monitorare l'esperienza online dei propri figli. Verso la componente studentesca: inserimento nel curricolo di temi legati alla affidabilità delle fonti online, all'interculturalità e al rispetto delle diversità. Qualora si venga a conoscenza di casi simili, occorre convocare i genitori per richiamarli a un maggiore controllo sulla fruizione di Internet da parte dei propri figli e/o sulla necessità di non usufruirne in presenza degli stessi.
Sexting e pedopornografia.	Verso i genitori: ❖ informazione circa le possibilità di attivare forme di controllo parentale della navigazione. Verso la componente studentesca: ❖ inserimento nel curricolo di temi legati all'affettività, alla sessualità e alle differenze di genere. ❖ In casi simili, se l'entità è lieve occorre in primo luogo parlarne con alunne e alunni e rispettivi genitori, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. ❖ Chi è immerso dalla nascita nelle nuove tecnologie spesso non è consapevole che una foto o un video diffusi in rete potrebbero non essere tolti mai più né è consapevole di scambiare o diffondere materiale pedopornografico. ❖ In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico per gli adempimenti del caso.
Violazione della privacy	Informazione sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farle rispettare. Se il comportamento rilevato viola solo le norme di buona convivenza civile e di opportunità, occorre convocare i soggetti interessati per informarli e discutere dell'accaduto e concordare forme costruttive ed educative di riparazione. Qualora il comportamento rappresenti un vero e proprio illecito, il Dirigente Scolastico deve esserne informato in quanto a seconda dell'illecito sono previste sanzioni amministrative o penali.

.