E-Safety Policy- in collaborazione con

1. **Introduzione**

1.1 Scopo della e-Policy

Il presente documento ha lo scopo di illustrare all'utenza scolastica le regole per un uso corretto e responsabile degli strumenti tecnologici collegati alla rete internet in uso nell'Istituto.

Si intende promuovere lo sviluppo della competenza digitale, che passa attraverso la conoscenza di procedure e competenze tecniche e di norme comportamentali, dettate da un uso consapevole e critico da parte degli alunni, delle tecnologie digitali e di internet. Lo scopo è di prevenire ed eventualmente rilevare e affrontare, situazioni derivanti da un uso pericoloso delle stesse.

Il primo passo è informare gli alunni dei rischi cui si espongono nella navigazione in rete, mentre dal canto suo l'Istituto si attiva per limitare l'accesso a siti potenzialmente dannosi, i cui contenuti possano risultare illegali o inadeguati. Gli insegnanti, infine, hanno il ruolo di guidare le attività on-line a scuola e illustrare le regole di comportamento per la navigazione in rete anche a casa.

Ai docenti, in particolare, spetta il ruolo di informare, piuttosto che censurare, gli alunni affinché imparino ad usare consapevolmente i contenuti e i servizi della rete per conoscere gli effetti cognitivi, comportamentali delle sue potenzialità oltre alle informazioni utili a gestire gli strumenti tecnologici.

Di seguito si schematizzano i rischi cui la comunità scolastica è sottoposta.

1.2 Rischi per gli utenti:

- valutazione di autenticità ed esattezza dei contenuti on-line;

- bullismo on-line;

- sexting (adescamento a scopo sessuale con invio di testi o immagini sessualmente esplicite);

- grooming (adescamento tramite manipolazione psicologica per ottenerne la fiducia ai fini dell'abuso sessuale);

- violazione della privacy e copyright;

- salute psicologica.

2. **Ruoli e Responsabilità:**

2.1 Dirigente Scolastico

Il Dirigente Scolastico è garante:

- dei dati e della sicurezza dei dati;

- di un accesso protetto e filtrato della rete internet;

- della formazione del personale sull'uso delle tecnologie informatiche;

- delle procedure da attuare in caso d'infrazione della e-Policy;

- dell'esistenza di un sistema di monitoraggio interno periodico della sicurezza on-line

2.2. Il Direttore dei Servizi Amministrativi

- assicura, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici in grado di garantire un corretto funzionamento dell'infrastruttura tecnica dell'Istituto, sicura rispetto ad un uso scorretto e ad attacchi esterni.

2.3. L'Animatore Digitale, il suo team, lo Staff

- promuovono una cultura per la salvaguardia e la sicurezza on line presso tutti gli utenti;

- si assicurano che tutto il personale sia a conoscenza delle procedure da seguire per la segnalazione e la gestione in caso d'infrazione della sicurezza on line e in caso di segnalazione e gestione di fenomeni di cyberbullismo, in tutte le sue forme;

- coordinano i contatti con le autorità locali e le autorità competenti;

- diffondono la conoscenza della e-safety presso la comunità scolastica.

2.4. I docenti

Ai docenti spetta il compito di:

- informarsi/aggiornarsi sulle tematiche relative alla sicurezza nell'utilizzo delle tecnologie digitali e di Internet e di rispettare il presente regolamento;

- assicurarsi che gli alunni rispettino la normativa sul copyright;

- garantire la riservatezza dei dati personali trattati ai sensi della normativa vigente;

- segnalare al D.S. qualsiasi difficoltà, bisogno o abuso da parte degli alunni, nell'utilizzo delle tecnologie digitali.

2.5. I collaboratori scolastici

- comprendono e contribuiscono e a promuovere la politica di e-safety della scuola;

- segnalano eventuali abusi nell'uso delle tecnologie digitali e di accesso a Internet.

2.6. Gli alunni

Agli alunni spetta il compito di:

- leggere, comprendere e rispettare il documento di e-safety;

- rispettare le norme sul diritto d'autore, evitando il plagio;

- segnalare abusi e condotte non adeguate rispetto ai contenuti on line;

- essere consapevoli che l'utilizzo delle tecnologie digitali deve essere sempre autorizzato dai docenti, sotto il cui controllo è sottoposto;

- essere consapevoli dei rischi cui incorrono nell'utilizzo di internet, soprattutto a casa;

- adottare comportamenti rispettosi degli altri anche nella comunicazione in rete;

- comunicare tempestivamente eventuali anomalie e difficoltà nell'utilizzo delle tecnologie digitali a docenti e genitori.

2.7. I genitori

I genitori collaborano con la scuola nel:

- sostenere la politica di salvaguardia di sicurezza on line;

- leggere, comprendere e controfirmare l'accordo di e-Policy con la scuola;

- seguire i suggerimenti e le condizioni d'uso delle TIC (Tecnologie per l'informatica e la comunicazione) indicate dai docenti anche nello studio a casa, controllandone l'utilizzo del PC e di internet da parte dei figli.

2.8 **Condivisione e comunicazione della e-Policy all'intera comunità scolastica**

La condivisione della e-policy avverrà attraverso la pubblicazione sul sito web della scuola dopo essere stata approvata dal Collegio dei Docenti. All'inizio del percorso scolastico di ogni ordine di scuola, la E-Policy viene illustrata ai genitori e, in modi opportuni in relazione all'età, agli alunni insieme al Patto di Corresponsabilità Educativa. Il contenuto del presente documento si applica a tutti i membri della comunità scolastica

3. **Gestione delle infrazioni alla e-Policy**

Per la natura stessa della comunicazione attraverso internet, non è possibile garantire che contenuti non idonei vengano visualizzati su un computer della scuola o su dispositivi mobili, non essendo possibile accertare responsabilità da parte della scuola o delle autorità preposte. Tuttavia gli utenti saranno informati sulle sanzioni in caso di infrazione della e-Policy, sempre rapportate all'età e al livello di sviluppo degli alunni, oltre che alla gravità dell'infrazione stessa. Le eventuali infrazioni potranno riguardare:

- un uso offensivo e lesivo della dignità propria e altrui della comunicazione in rete;

- comportamenti connessi al sexting;

- l'utilizzo delle tecnologie informatiche e dei dispositivi mobili non autorizzati dal docente;

- l'accesso a siti internet non autorizzati dal docente

Le possibili infrazioni del personale docente sono così di seguito schematizzate:

- utilizzo delle tecnologie della scuola, d'uso comune con gli alunni;

- utilizzo delle comunicazioni elettroniche con genitori e alunni;

- violazione della privacy nel trattamento dei dati personali degli alunni;

- diffusione delle password;

- mancata informazione degli alunni sul corretto e responsabile uso di tecnologie e strumenti informatici e di internet;

- mancata vigilanza nell'utilizzo degli stessi

- mancata segnalazione di situazioni critiche relativamente alla condotta degli alunni rispetto alla e-Policy d'istituto.

Le procedure di sanzione sono quelle previste dalla legge e dai contratti di lavoro.

4. Integrazione della e-Policy con Regolamenti esistenti.

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

5. Norme generali per l’utilizzo del Laboratorio di Informatica

- Agli allievi, agli esterni ed al personale non preposto non è consentito accedere ai siti in cui sono custoditi dati e/o informazioni sensibili.
- La richiesta ed il conseguente spostamento di apparecchiature multimediali in altro laboratorio o in aula, se non previsto nel piano orario di utilizzo, deve essere rivolta con congruo anticipo al Responsabile.
- Non è possibile cambiare di posto le tastiere, le stampanti, i mouse, le casse o qualunque altra attrezzatura senza autorizzazione.
- Il personale e gli allievi dovranno aver cura di rispettare le procedure corrette di accensione, di utilizzo e di spegnimento delle macchine. Non è consentito consumare pasti o bevande nel laboratorio.

- E' possibile l'utilizzo di periferiche I/O personali solo previa autorizzazione.
- L'uso delle stampanti va effettuato solo a conclusione del lavoro ed è subordinato ad una preventiva anteprima di stampa avendo cura di evitare spreco di carta e d'inchiostro.
- Prima di uscire dal laboratorio occorre accertarsi che le sedie siano al loro posto e che non vi siano cartacce o rifiuti. Il docente dell'ultima classe o corso che utilizza il laboratorio dovrà accertarsi che tutte le apparecchiature elettriche siano spente e riordinate nell'apposito armadio avendo cura che siano posti sotto carica.
- Per motivi di manutenzione ordinaria e/o straordinaria, i PC possono essere formattati, si consiglia pertanto di salvare i dati utilizzando apposite piattaforme o sistemi on line.
- Periodicamente si provvederà a coordinare l'aggiornamento del software antivirus e a verificare la consistenza dei firewall.
- La violazione del presente Regolamento potrà comportare la temporanea o permanente sospensione dell'accesso al laboratorio.

6. **E-Policy d'Istituto**

- Gli utenti possono utilizzare le postazioni dell'Istituto per accedere in Internet solo per scopi didattici o collegati alle attività di lavoro degli uffici.
- I software installati sono ad esclusivo uso didattico. Chiunque abbia bisogno di aggiornamenti o nuovi applicativi da acquistare deve farne richiesta all'Animatore Digitale.
- Non è possibile effettuare copie del software presente nelle postazioni salvo autorizzazione solo nel caso si tratti di free software.
- Non è consentito modificare le configurazioni hardware e software delle apparecchiature, senza autorizzazione. Ogni aggiornamento e installazione di nuovi componenti (software, hardware o linee di comunicazione dati) viene registrato.
- È espressamente vietata qualsiasi azione tesa a superare il blocco delle password di BIOS o di livello di amministratore.
- Non è possibile utilizzare e/o installare software diverso da quello di cui la scuola è regolarmente dotata di licenza di utilizzo. Si richiama l'osservanza delle norme per il rispetto del diritto d'autore e del copyright.
- Non sono consentite azioni tese a superare le protezioni applicate ai sistemi. E' vietato adottare comportamenti che possano interferire con la privacy e con la libertà di espressione.
- Il software reperibile sulla rete può essere coperto da brevetti e/o vincoli di utilizzo di varia natura. Leggere sempre attentamente la documentazione di

accompagnamento prima di utilizzarlo, modificarlo o ridistribuirlo in qualunque modo e sotto qualunque forma.

- In rete occorre sempre rispettare tutti i vincoli di legge.
- Comportamenti palesemente scorretti da parte di un utente, quali violare la sicurezza di archivi e computer della rete, violare la privacy di altri utenti della rete leggendo o intercettando la posta elettronica loro destinata, compromettere il funzionamento della rete e degli apparecchi che la costituiscono, con programmi (virus, trojan horses, ecc.) costruiti appositamente, costituiscono dei veri e propri crimini elettronici e come tali sono punibili.

7. **Account**

- Gli utenti che otterranno un account per l'ingresso nella rete d'Istituto dovranno prendere visione ed accettare il presente Regolamento.
- Il personale può acquisire il diritto all'accesso alla rete completo, locale o remoto, previa autorizzazione del DS.
- Verificata la disponibilità di prese per la connessione fisica e di indirizzi di rete, qualunque dipendente dell'istituto può richiedere di connettere alla rete locale dell'Istituzione Scolastica altri calcolatori utili per le proprie attività didattiche.
- Tutti i dipendenti con incarichi di responsabilità, docenti, assistenti e collaboratori, secondo disponibilità e previa autorizzazione del Dirigente Scolastico, possono richiedere un account di posta elettronica.
- Chiedere un account comporta l'accettazione implicita delle norme d'uso per le macchine comuni, e delle norme previste nei commi precedenti.

8. **Internet e Password**

- Gli utenti utilizzano le connessioni a Internet esclusivamente per le necessità di ufficio o di didattica, escludendo ogni e qualsiasi attività di uso privato e/o per conto terzi, in qualsiasi modo effettuate.
- Gli utenti sono responsabili dell'uso dell'account loro assegnato.
- Gli utenti non devono diffondere messaggi di posta elettronica di provenienza dubbia, non partecipano a sequenze di invii di messaggi ("catena di S. Antonio") e non inoltrano o diffondono messaggi che annunciano nuovi virus o altri pericoli per le apparecchiature.
- E’ vietato aprire allegati provenienti da fonti non conosciute o con estensione .exe, .combat.
- È vietato l'uso di servizi di comunicazione che esulino dalle normali e prevedibili funzioni di scambio di posta elettronica, browsing (http) e trasferimento di file (ftp).

In particolare si fa esplicito divieto di installare programmi che utilizzino servizi di connessione Internet non usuali, come servizi di chat e messaggistica (p.e. IRC, ICQ), scambio di file particolari (p.e. mp3) e simili.

- Il Responsabile coordina la configurazione del software di navigazione dei client utilizzati dagli alunni in maniera da rendere possibile il monitoraggio e il filtraggio della navigazione operata da un proxy server e impedendo la consultazione di siti proibiti.
- E' vietato alterare le opzioni del software di navigazione.
- Il servizio di Internet viene utilizzato, da parte degli allievi interessati, solo per scopi didattici e di ricerca.
- L'Istituzione Scolastica possiede un sito web per il quale è stato nominato un Referente. E' possibile richiedere la pubblicazione sul sito di rubriche o pagine: la richiesta verrà vagliata ed eventualmente autorizzata dal DS.
- Prima di scaricare documenti o file da Internet chiedere al docente d'aula.
- Chiedere l'autorizzazione al Responsabile per sottoscrivere una newsletter.
- Gli utenti devono necessariamente attivare credenziali e password per accedere agli account richiesti.

9. **Procedure di sicurezza per le attività svolte nel Laboratorio di Informatica**

- Questa procedura deve essere letta dai rispettivi insegnanti a tutte le classi all'inizio dell'anno scolastico e affisso in modo ben visibile all'interno del laboratorio.
- L'accesso al laboratorio è vietato al personale non addetto e agli allievi non accompagnati dal personale.
- Al fine di ridurre sensibilmente il rischio di incidenti durante le attività svolte, gli insegnanti sono chiamati ad osservare e far rispettare agli allievi le norme sotto riportate.

I Docenti che utilizzano il laboratorio sono invitati a:

- riportare sul registro delle presenze il nome, la data, l'ora, la classe ed eventuali segnalazioni in merito allo stato dell'aula e delle apparecchiature.
- non sistemare sgabelli, sedie o poltroncine lungo le vie di fuga per non intralciare ed ostacolare per un eventuale esodo in caso di emergenza adottare le opportune norme di sicurezza nell'uso delle attrezzature presenti in laboratorio
- osservare le norme di sicurezza e di evacuazione predisposte ai fini della sicurezza individuale e collettiva, facendo riferimento al Piano di Emergenza affisso nel laboratorio

- vigilare affinché non venga modificata in alcun modo la configurazione sia dei computer sia degli applicativi in essi installati
- controllare che non vengano installati software senza autorizzazione
- vigilare affinché non vengano danneggiati mouse, tastiere, stampanti e altri dispositivi
- assicurare massima sorveglianza e non lasciare mai le classi senza sorveglianza.

Gli studenti che accedono al laboratorio sono invitati a:

- non creare intralcio o confusione agli altri studenti, in corridoio, nell'attesa di entrare in laboratorio;
- avere un comportamento corretto e rispettoso delle persone e delle apparecchiature in esso presenti, simile a quello richiesto in qualsiasi altro ambiente scolastico;
- comunicare tempestivamente all'insegnante eventuali manomissioni, danni o irregolarità riscontrati nell'aula o nelle attrezzature;
- non utilizzare alcuna apparecchiatura, macchina, dispositivo o attrezzatura senza l'autorizzazione esplicita dell'insegnante;
- non modificare la configurazione dei computer e dei pacchetti di software in esso installati;
- non utilizzare i servizi internet senza il permesso esplicito dell'insegnante;
- non utilizzare i computer per giochi elettronici.

10. Formazione e Curricolo

10.1 Curricolo sulle competenze digitali per gli studenti.

L'Istituto integra il curricolo scolastico con attività educative che favoriscano la cultura della sicurezza on line. In tal senso si impegna a sviluppare una serie di competenze e comportamenti adeguati alle età degli alunni, tra cui:

- programmare attività e far partecipare gli alunni a laboratori di Coding in occasione della Settimana del codice;
- sviluppare una serie di strategie per valutare e verificare le informazioni prima di accettare l'esattezza, sviluppando il pensiero critico;
- utilizzare software per la presentazione di dati;
- assumere comportamenti adeguati in ambienti on line, rispettosi della dignità propria e altrui;

- essere consapevoli che dati personali e fotografie possono essere manipolate e usate in maniera fraudolenta e lesiva da parte di terzi;
- comprendere che le "identità virtuali" possono essere ingannevoli;
- capire il motivo per cui non devono pubblicare foto o video di altri senza il loro permesso;
- conoscere le norme in materia di copyright;
- sviluppare una sempre maggiore sensibilità verso l'impatto che il cyberbullismo, sexting e grooming posso avere sulla vita propria e dei compagni e sapere a chi rivolgersi per segnalare abusi connessi all'utilizzo di internet;
- utilizzare con attenzione Internet per garantire che si adatti alla loro età e sia di sostegno agli obiettivi di apprendimento per le aree curricolari specifiche.

10.2 **Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali**

In attuazione del PNSD questo Istituto ha realizzato:

- individuazione e formazione di un Animatore Digitale;
- formazione dei docenti all'utilizzo del registro elettronico e dello scrutinio elettronico;
- somministrazione di un questionario rivolto ai docenti per la rilevazione dei bisogni "digitali";
- ricognizione e messa a punto delle dotazioni digitali;
- attivazione e comunicazione di iniziative di formazione, in particolare rivolte allo sviluppo e alla diffusione del Coding e del pensiero computazionale.

La scuola ha previsto:

- una politica di informazione e diffusione della e-safety d'Istituto;
- attivazione di Google Suite for Education.

10.3 Sensibilizzazione delle famiglie.

L' Istituto s'impegna a promuovere una cultura dell'informazione, volta a coinvolgere le famiglie nella cultura di un uso consapevole delle tecnologie digitali e di internet, attraverso:

- conoscenza e condivisione del Regolamento della e-Policy, al fine di garantire che i principi di comportamento sicuro on-line siano chiari;
- informazione attraverso il sito della scuola;

- incontri di consulenza con esperti;
- fornire informazioni sui siti nazionali di sostegno per i genitori, quali il sito www.generazioniconnesse.it

11. Gestione dell’infrastruttura e della strumentazione ICT della scuola.

Data la giovane età degli studenti del nostro istituto è fondamentale fare tutto il possibile per evitare l’esposizione a contenuti inappropriati

- Accesso ad internet: filtri antivirus e sulla navigazione, gestione accessi (password, backup, ecc.), e-mail.

I contenuti didattici, le informazioni alle famiglie, le comunicazioni al personale sono pubblicati sul sito web dell'Istituto/RE, sotto la supervisione dal D.S., nel rispetto delle norme vigenti sulla privacy e del PTTI d'Istituto.

- Sicurezza Rete Lan

L'Istituto dispone di una rete locale (rete segreteria) cui accedono i computer dell' amministrazione, isolata dal resto della rete di Istituto (rete didattica). Il collegamento di computer portatili o palmari personali alla rete di Istituto deve essere autorizzato dal Dirigente Scolastico.

- La rete interna è protetta da Firewall per quanto riguarda le connessioni con l'esterno. Le postazioni sono protette con sistemi antivirus.

- Sicurezza della rete senza fili (Wireless –WiFi)

L'Istituto dispone di una rete con tecnologia senza fili. L'accesso alla rete wireless è autorizzato ai docenti dal D.S., tramite password e riconoscimento del dispositivo utilizzato. Le regole di comportamento sono analoghe a quelle per la connessione alle reti cablate di Istituto.

12. Strumentazione personale

PER GLI STUDENTI

Agli studenti delle Scuole primarie è vietato l'utilizzo di cellulari per l'intera durata delle attività scolastiche.

Agli studenti della Scuola secondaria di primo grado è vietato l'utilizzo di cellulari per l'intera durata delle attività scolastiche (intervalli inclusi). È consentito agli alunni con Bisogni Educativi Speciali utilizzare notebook o tablet forniti dalla scuola. È consentito a tutti gli alunni, in casi specifici concordati con il docente (uscite didattiche, produzioni multimediali...), l'utilizzo di dispostivi elettronici personali per scopi didattici.

PER I DOCENTI

Ai docenti durante l’orario di servizio è consentito l'utilizzo di dispositivi elettronici personali solo ed esclusivamente per fini didattici.

PER IL PERSONALE ATA

Di norma ai collaboratori scolastici è vietato l'utilizzo di dispositivi elettronici durante l'orario di servizio.

13. Prevenzione, rilevazione e gestione dei casi

I rischi cui un allievo può incorrere a scuola nell’utilizzo delle TIC derivano da un uso non corretto del telefono cellulare personale o dello smartphone, dei pc della scuola collegati alla rete. Eludendo la sorveglianza degli insegnanti, gli allievi potrebbero incorrere in tutti i rischi connessi all'uso scorretto di internet, tra cui i più comuni:

- cyberbullismo
- sexting
- adescamento
- gioco d'azzardo

Tra questi il cyberbullismo si sviluppa, in ambiente scolastico, a partire da prepotenze riportate nel contesto virtuale di internet. Esso si manifesta attraverso invio di sms, mms, e mail offensivi/e o di minaccia, diffusione di messaggi offensivi ai danni della vittima, attraverso la divulgazione di sms o e-mail o nelle chat, pubblicazione di foto o filmati che ritraggono prepotenze sulle vittime. Tale fenomeno, sempre più diffuso e pervasivo, può essere seriamente prevenuto solo attraverso la diffusione di una seria cultura dell'inclusione, cui il PTOF dell'Istituto è improntato.

13.1 Azioni di prevenzione

Le azioni previste di prevenzione nell’utilizzo delle TIC sono le seguenti:

- Informare i docenti, i genitori, il personale ATA e gli studenti sui rischi che un uso non sicuro delle nuove tecnologie può favorire, anche attraverso attività mirate alla conoscenza del fenomeno del bullismo e del cyberbullismo;

- creare degli spazi in cui gli alunni si possano confrontare su questo tema, utilizzando come spunti di riflessione: filmati, canzoni, ecc.

- confrontarsi con gli altri insegnanti della classe, della scuola o con esperti del territorio;

- rivolgersi al portale (www.generazioniconnesse.it).;

- Consentire l’utilizzo del cellulare solo per scopi didattici e sotto il controllo dei docenti;

- Utilizzare filtri, software che impediscono il collegamento ai siti web per adulti (black list)

13.2 Contenuti “pericolosi”

I contenuti “pericolosi” per gli alunni possono essere i seguenti:

- contenuti che violino la privacy (foto e informazioni personali, l'indirizzo di casa o il numero di telefono);

- 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 che implichino la sfera della sessualità.

13.3 Modalità di segnalazione

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;
- comunicazione scritta al Dirigente scolastico.

Per i reati più gravi 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.

13.4 Rilevazione e gestione dei casi

Si considerano da segnalare tutte quelle situazioni che si configurano come episodi di cyber bullismo (caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona o un piccolo gruppo tramite un utilizzo irresponsabile dei social network), ma anche usi inappropriati della rete (siti d’odio, contenuti non adatti all’età degli alunni…).

I docenti di classe informano il Dirigente Scolastico, il quale procede ad informare le famiglie. Tutte le segnalazioni riportate dai docenti vengono registrate su apposita scheda

- Per una efficace gestione dei casi la scuola si riserva di utilizzare lo schema messo a disposizione sul sito www.generazioniconnesse.it