

## E-Safety Policy DELLA Scuola Secondaria di Primo Grado "L. Castiglione" – Bronte



SCUOLA SECONDARIA DI 1° GRADO STATALE "L. CASTIGLIONE"

Piazza Avv. Vincenzo Castiglione, 2 – 95034 Bronte (Ct)

TEL. 095/691180 FAX 095/7725146

c.m. ctmm119008 - cod. fisc. 80011270875

e.mail [ctmm119008@istruzione.it](mailto:ctmm119008@istruzione.it) pec [ctmm119008@pec.istruzione.it](mailto:ctmm119008@pec.istruzione.it)

SSPG "L. CASTIGLIONE" - BRONTE  
Prot. 0003267 del 11/06/2021  
(Uscita)

### Introduzione

Lo sviluppo e l'integrazione dell'uso delle ICT nella didattica, nonché la presenza sempre più diffusa delle tecnologie digitali nella vita di tutti i giorni, pone nuove attenzioni dal punto di vista del loro uso sicuro e consapevole. Vi sono numerose evidenze scientifiche sui benefici che l'uso delle tecnologie digitali possono apportare nel processo di insegnamento /apprendimento.

È compito dell'intera comunità scolastica, genitori inclusi, garantire che gli studenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato.

È in questo quadro che si inserisce la necessità di dotare la scuola di una propria *Policy di E-safety*, nell'ottica della gestione delle infrazioni attraverso il monitoraggio continuo della *Policy* e dell'integrazione con il *Regolamento d'istituto*.

Obiettivo del documento è quello di educare e sensibilizzare l'intera comunità scolastica all'uso sicuro e consapevole di *Internet* in conformità con le *Linee di orientamento* per azioni di prevenzione e di contrasto al *cyber bullismo* elaborate dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con il *Safer Internet Center* per l'Italia, programma comunitario istituito dal Parlamento Europeo e dal Consiglio dell'Unione. Il documento potrà essere revisionato annualmente.

### Scopo della Policy

Questa *policy* si applica a tutti i membri della comunità scolastica che hanno accesso o che sono utenti dei sistemi informatici della scuola.

In particolare essa viene redatta per regolare il comportamento della componente

studentesca dentro le aule scolastiche e per sensibilizzarli all'adozione di buone pratiche quando sono fuori dalla scuola e autorizza i membri del personale docente a erogare sanzioni disciplinari per comportamenti inappropriati avvenuti all'interno dell'istituzione scolastica. Questo è il caso degli episodi di cyberbullismo come di altri fenomeni di cui si tratta nella presente politica, che possono avvenire al di fuori della scuola, ma che sono legati alla frequentazione della stessa.

Il nostro Istituto accoglie minori "nativi digitali" che, fin dall'infanzia, sono esposti a rischi di cui sono inconsapevoli ,pertanto la scuola attua parallelamente attività di prevenzione, controllo e formazione di allieve, allievi e famiglie allo scopo di ridurre al minimo l'occorrenza di atti che non solo creano disagio nella comunità scolastica, ma possono configurarsi come reati.

La scuola opera in stretto collegamento con le autorità competenti e con istituzioni del settore educativo, per mettere in campo strategie di prevenzione al cyberbullismo e interventi di recupero nel caso in cui vengano individuati tali fenomeni, informando i genitori/tutori e chiedendo la loro collaborazione anche qualora gli episodi si siano verificati al di fuori delle attività didattiche.

## **Ruoli e responsabilità**

Si individuano 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 l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on line.

### Animatore Digitale, supportato dal Team per l'innovazione digitale:

- Stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale"e fornire 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 ed Internet a scuola, e proporre soluzioni metodologiche e tecnologiche, innovative e sostenibili,da diffondere nella scuola;
- coinvolgere la comunità scolastica (alunni, famiglie, e altri attori del territorio)nella partecipazione ad attività e progetti attinenti la"scuola digitale".

Direttore dei Servizi generali ed 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:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto;
- 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);
- sensibilizzare gli alunni a seguire le norme di sicurezza nell'utilizzo del web e utilizzare correttamente le tecnologie digitali.
- Segnalare eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste nel Regolamento d'istituto in caso di violazioni;
- Mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici;
- Controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche ecc. nelle lezioni e nelle altre attività scolastiche che ne prevedono la necessità a scopi didattici;
- Assicurarci che tutti gli studenti e le studentesse depositino il proprio dispositivo digitale spento nell'armadio di classe o nel cassetto della cattedra o nei casellari installati in prossimità dei corridoi al loro ingresso a scuola, consegnandolo 5 minuti prima il suono della campanella;
- Guidare la navigazione di studentesse e studenti, nelle lezioni in cui l'uso di Internet è pianificato, verso siti controllati come idonei per il loro uso, onde evitare di incontrare materiali inadatti.

Personale ATA:

- Avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- Aver letto e compreso la presente *policy*;

- Segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'Animatore digitale per le opportune indagini/azioni/sanzioni;
- Mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici;

Alunni:

- Non utilizzare dispositivi personali durante le attività didattiche se non espressamente consentito dal personale docente;
- Essere responsabili, in relazione al proprio grado di maturità e di apprendimento, 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 ICT;
- Comprendere l'importanza di adottare buone pratiche di sicurezza *on lin* e quando si utilizzano le tecnologie digitali per non correre rischi;
- Adottare condotte rispettose degli altri anche quando si comunica in rete;
- Avere una buona comprensione delle possibilità di ricerca sul web e della necessità di evitare il plagio, rispettare le normative sul diritto d'autore, non diffondere dati personali;
- comprendere l'importanza della segnalazione di ogni abuso, uso improprio o accesso a materiali inappropriati e conoscere il protocollo per tali segnalazioni;
- conoscere e comprendere le politiche sull'uso di dispositivi mobili e di macchine fotografiche digitali;
- capire le politiche di utilizzo delle immagini ed essere consapevoli del significato e della gravità del cyber-bullismo;
- capire l'importanza di adottare buone pratiche di sicurezza informatica in tutti i momenti della vita, a tutela dell'incolumità propria e altrui e per evitare di perpetrare reati punibili sia a livello scolastico sia da parte delle autorità competenti.

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.

**Condivisione e comunicazione della policy all'intera comunità scolastica**

Condivisione e comunicazione della Policy agli alunni

Nel corso dell'anno saranno dedicate alcune lezioni, tenute dai docenti individuati all'interno dei singoli Consigli di Classe, 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 dagli 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.

#### 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

[www.scuolacastiglione.edu.it](http://www.scuolacastiglione.edu.it) .

### **Gestione delle infrazioni alla policy**

Le potenziali infrazioni a carico degli alunni sono identificabili in:

- uso di *social network* e *blog* per pubblicare, condividere o, in genere, postare commenti o giudizi offensivi della dignità altrui
- condivisione di dati personali che possano permettere l'identificazione
- connessioni a siti proibiti o comunque non autorizzati
- pubblicazione di foto o immagini non autorizzate e/o compromettenti.

Gli interventi correttivi previsti per gli alunni saranno rapportati all'età e al livello di sviluppo del discente. Un primo intervento viene attuato dal docente secondo le modalità indicate:

- richiamo verbale;
- richiamo verbale con annotazione disciplinare sul registro e sul diario personale;
- convocazione della famiglia.

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 o al profilo professionale, 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 garantisca un'adeguata protezione degli stessi;
- diffusione delle *password* assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi.

Il Dirigente scolastico può controllare l'utilizzo delle ICT per verificarne la conformità alle regole di sicurezza, come l'accesso a Internet, ma non alla posta elettronica personale, procedere alla cancellazione di materiali inadeguati, o non autorizzati dal sistema informatico della scuola, conservandone una copia per eventuali successive investigazioni come in caso di contenzioso.

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

#### Disciplina dei genitori

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

Le situazioni familiari meno favorevoli sono:

- 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.

#### **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 per un uso efficace e consapevole del digitale nella didattica:

- PTOF
- Regolamento interno d'Istituto

## **Formazione e Curricolo**

Il Piano Nazionale Scuola Digitale (PNSD) ha l'obiettivo di modificare gli ambienti di apprendimento per rendere l'offerta formativa di ogni istituto coerente con i cambiamenti della società della conoscenza e con le esigenze e gli stili cognitivi delle nuove generazioni. Il PNSD, con valenza pluriennale, è quindi un'opportunità per innovare la Scuola, adeguando non solo le strutture e le dotazioni tecnologiche a disposizione dei docenti e dell'organizzazione, ma soprattutto le metodologie didattiche e le strategie usate con gli alunni in classe.

Il D.M.851 del 27 ottobre 2015, ai sensi dell'art.1, comma 56 della legge 107/2015, ne ha previsto l'attuazione al fine di:

- Migliorare le competenze digitali degli studenti anche attraverso un uso consapevole delle stesse;
- Implementare le dotazioni tecnologiche della scuola al fine di migliorare gli strumenti didattici e laboratori ali ivi presenti;
- Favorire la formazione dei docenti sull'uso delle nuove tecnologie ai fini dell'innovazione didattica;
- Individuare un Animatore Digitale e un Team per l'innovazione digitale che supporti adeguatamente l'innovazione didattica, nonché l'attività dell'Animatore Digitale.

## **Curricolo sulle competenze digitali degli studenti**

Nell'ambito del PNSD questa scuola si propone un programma di progressiva educazione alla sicurezza online come parte del curriculum scolastico. Si impegna a sviluppare una serie di competenze e comportamenti adeguati alle età degli alunni ed esperienza tra cui:

- programmare attività e far partecipare gli alunni a laboratori di Coding e/o ad attività legate alla sicurezza online;
- sviluppare una serie di strategie per valutare e verificare le informazioni prima di accettarne l'esattezza;
- essere a conoscenza che l'autore di un sito/pagina web può avere un particolare pregiudizio;
- sapere come restringere o affinare una ricerca;
- capire il comportamento accettabile quando si utilizza un ambiente on line, vale a dire essere educato, non utilizzare comportamenti inappropriati, mantenerle informazioni personali private;
- capire il motivo per cui non devono pubblicare foto o video di altri senza il loro permesso;
- sapere di non scaricare alcun file come i file musicali senza permesso;
- comprendere l'impatto di bullismo online e sapere come cercare aiuto se sono in pericolo;

- sapere come segnalare eventuali abusi tra cui bullismo online e come chiedere aiuto ai docenti e ai genitori;
- utilizzare con attenzione Internet per garantire che si adatti alla loro età e supporti gli obiettivi di apprendimento per le aree curriculari specifiche.

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

Nell'ambito del PNSD questo Istituto ha previsto:

- individuazione e formazione di un Animatore Digitale che come docente accompagnerà il Dirigente e il DSGA nell'attuazione degli obiettivi e delle innovazioni previste dal PNSD;
- formazione dei docenti del Team per l'innovazione digitale;
- formazione dei docenti sull'utilizzo del Registro Elettronico e dello Scrutinio Elettronico;
- ricognizione e messa a punto delle dotazioni digitali;
- comunicazione di iniziative di formazione;
- condivisione con tutto il personale di informazioni e indicazioni in materia di sicurezza online attraverso il sito web.

### **Sensibilizzazione delle famiglie**

Questo Istituto esegue un programma di consulenza, orientamento e formazione per i genitori attraverso le seguenti azioni:

- comunicare ai genitori e fornire informazioni sulla normativa vigente sui comportamenti devianti on line attraverso pubblicazioni sul sito web della scuola;
- fornire informazioni sui siti nazionali di sostegno per i genitori, quali il sito [www.generazioniconnesse.it](http://www.generazioniconnesse.it)

### **Gestione dell'infrastruttura e della strumentazione ICT della scuola**

#### Accesso ad internet

Ai docenti è consentito accedere ad Internet da propri dispositivi utilizzando l'hotspot dell'Istituto, tramite login e password personale fornita dal Dirigente Scolastico.





Pagina di accesso all'hotspot della Scuola Castiglione

Il Regolamento di Istituto vieta agli alunni l'uso del cellulare e in particolare non è consentito accedere ad Internet da propri dispositivi utilizzando l'hotspot della scuola. Pertanto, è severamente vietato lasciare le password personali incustodite o dare la password personale agli alunni per accedere all'hotspot della scuola .

I pc della Segreteria dispongono di antivirus con licenza e sono regolarmente aggiornati.

#### 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.

#### Sito web della scuola

L'Istituto dispone di un proprio spazio web e la gestione del sito risponde alla normativa per quanto riguarda i contenuti (accuratezza, appropriatezza, aggiornamento).

La scuola detiene i diritti d'autore dei documenti che si trovano sul proprio sito o di quei documenti per i quali è stato chiesto ed ottenuto il permesso d'autore proprietario.

Le informazioni pubblicate sul sito della scuola relativa alle persone da contattare rispetteranno le norme vigenti sulla privacy.

La scuola, in qualità di ente pubblico, pubblicherà sul proprio sito web i contenuti che saranno valutati come pertinenti alle finalità educative istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative.

#### Social network

Per la Legge l'utilizzo dei Social Network con la pubblicazione di nomi e giudizi sulle persone o sulle istituzioni e la diffusione di foto/filmati senza il consenso e, comunque, all'insaputa delle persone coinvolte può determinare ricadute di carattere anche penale, come ad esempio la diffamazione.

Si invitano pertanto tutti gli studenti a non prelevare o diffondere immagini, video o registrazioni anche solo audio, non autorizzate, ed eliminare da Internet eventuali riferimenti offensivi o comunque illeciti (ed inopportuni) nei confronti dell'Istituto e dei suoi docenti e studenti.

Allo stesso tempo, si invitano gli allievi e i genitori a fare un uso prudente dei Social Network, in particolare Facebook e Whatsapp, limitando nell'uso alle sole comunicazioni funzionali, evitando ad ogni modo di esprimere giudizi che una volta pubblicati comportano sempre una assunzione di responsabilità da parte di chi li ha scritti o anche semplicemente diffusi.

### **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 necessari e 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.

### **Strumentazione personale**

*Per gli studenti: gestione degli strumenti personali - cellulari, tablet, etc....*

Come espresso nel Patto di corresponsabilità, gli alunni si impegnano a tenere spenti e custodire i propri cellulari ( SPENTI) nel cassetto della cattedra, o armadio, o casellari installati nei corridoi i propri dispositivi personali; 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.

Per quanto riguarda l'utilizzo dei tablet, questi possono essere utilizzati solo alla presenza del docente e per ragioni prettamente scolastiche.

Non è consentito l'uso di dispositivi personali.

*Per I docenti: gestione degli strumenti personali cellulari, tablet, etc....*

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.

Per il personale della scuola: gestione degli strumenti personali cellulari, tablet, etc.

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.

## **Prevenzione, rilevazione e gestione dei casi**

### **Rischi**

Al personale che opera nella scuola, e in modo particolare agli insegnanti, viene oggi offerta la possibilità di essere promotori e garanti della costruzione dialogica di un percorso formativo partecipato, ma il loro ruolo diventa spesso inevitabilmente quello di confidenti degli alunni e delle loro esperienze. Proprio per questo, gli insegnanti sono anche investiti del ruolo di sorta di "torre di avvistamento", avamposto privilegiato delle problematiche e dei rischi che bambini e adolescenti possono trovarsi ad affrontare ogni giorno. Basti pensare all'elevato numero di casi di bullismo e di cyber bullismo che gli insegnanti si trovano ad affrontare durante il loro insegnamento quotidiano.

La prima responsabilità degli insegnanti consiste, dunque, 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&Moon2010)

**adescamento o grooming:** una tecnica di manipolazione psicologica, che gli adulti potenzialmente 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 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, quasi tutti gli studenti portano a scuola i dispositivi che dovrebbero

tenere spenti durante la lezione. 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.

## **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, la scuola si impegna a:

- diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web, condividendo materiali del progetto "Generazioni connesse" messi a disposizione sul sito web.
- 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 e smartphone, agli studenti in orario scolastico, se non per esplicite attività didattiche e sotto la supervisione del docente proponente. 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.

I docenti si impegnano a:

Accompagnare gli alunni nella navigazione in rete, coinvolgendoli nell'esplorazione delle opportunità e dei rischi

approfondire, con attività mirate in classe, la conoscenza del fenomeno del bullismo e cyberbullismo

I genitori si impegnano a:

- firmare il patto educativo di Corresponsabilità
- prendere visione della ESafety Policy messa a disposizione di docenti, famiglie ed alunni sul sito della scuola
- seguire le azioni promosse dalla scuola per un uso corretto

della rete

Gli alunni si impegnano a:

- prendere visione del Patto educativo di corresponsabilità che i genitori hanno firmato
- prendere visione della ESafety Policy pubblicata sul sito web della scuola
- rispettare le regole per un uso corretto della tecnologia
- denunciare qualsiasi caso di abuso online
- prendere parte a qualsiasi evento che la scuola organizza in materia di sicurezza online

### **Rilevazione e gestione dei casi**

Intervenire in situazioni di sicurezza online non è mai semplice e per tale motivo la scuola si impegna ad individuare due strumenti che potranno agevolare l'intera comunità scolastica:

- nel decidere come intervenire
- nel tenere traccia di ciò che è avvenuto rispetto ai comportamenti degli alunni online e di come è stato gestito il problema.

L'obiettivo a lungo termine, che come comunità scolastica ci diamo, è quello di creare una memoria condivisa non solo di ciò che accade nella scuola rispetto al web, ma anche di strutturare una fonte esemplificativa che possa orientare sempre più e sempre meglio le azioni di contrasto ad episodi che, nel tempo, potrebbero ripetersi.

Ogni volta che un membro del personale o studente violata ESafety Policy, la decisione finale sul livello di sanzioni sarà a discrezione del Dirigente Scolastico e rifletterà le procedure disciplinari della scuola così come previsto nel Regolamenti di Istituto.

Approvato dal Collegio dei Docenti con delibera n. 42 del 17/05/2021

Approvato dal Consiglio d'Istituto con delibera n. 109 del 18/05/2021

