MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITA', DELLA RICERCA

Istituto Comprensivo Statale "Galluppi-Collodi-Bevacqua"

Via Botteghelle n° 1- 89132 Reggio Calabria Tel/fax 096551066/0965 599120

C.M. RCIC87200P - rcic87200p@istruzione.it - rcic87200p@pec.istruzione.it – www.icgalluppirc.gov.it – Codice fiscale 92081300805

E-Safety Policy

INDICE

1. Introduzione

1.1. Premessa

Sia a livello internazionale, che nel contesto italiano, la presenza sempre più diffusa delle tecnologie digitali nella vita di tutti i giorni dei più giovani, compresi gli ambienti scolastici, apre nuove opportunità ma pone nuove attenzioni dal punto di vista del loro uso sicuro, consapevole e positivo. Inoltre, lo sviluppo e l'integrazione dell'uso delle TIC, ed in particolare di internet, nella didattica, offrono le condizioni e l'occasione per una trasformazione dell'insegnamento e dell'apprendimento nelle scuole e a tale proposito esistono numerose evidenze scientifiche sui benefici che l'uso delle tecnologie digitali possono apportare a tali aspetti. Ciò pone però delle sfide importanti, che riguardano più livelli di conoscenze, abilità e attitudini che i più giovani hanno bisogno di sviluppare, nell'ottica di accrescere le competenze digitali.

Gli adulti hanno un ruolo fondamentale nel garantire che bambini/e e adolescenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato e sicuro, ruolo che vede coinvolti a pieno titolo tutti coloro che hanno un ruolo educativo, oltre che formativo, in altre parole la comunità scolastica nel suo complesso, genitori inclusi.

E' in questo quadro che si inserisce la necessità di affrontare la questione da più punti di vista e interessando più interlocutori, inclusi i più giovani, per arrivare a dotare ogni comunità scolastica di una propria Policy di E-safety.

1.2. Scopo della Policy

Con il termine *Policy* si intende un insieme di regolamenti, linee di azione e attività poste in essere per fare fronte ad una serie di necessità individuate. Una policy non è mai il risultato di un'azione unica, quanto piuttosto l'esito delle interazioni di un insieme di azioni e decisioni.

Il presente documento ha quindi lo scopo di descrivere:

- Le norme comportamentali e le procedure per l'utilizzo delle ICT nell'Istituto Comprensivo
- 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 ha prodotto un Piano d'Azione che individua il percorso e le risorse necessarie per elaborare e implementare una Policy di E-Safety, 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.

1.3. Comunicazione e condivisione della Policy all'interno della comunità scolastica

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) 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 tramite pubblicazione sul sito web della scuola e sul diario scolastico;
- 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

Infrazione degli alunni

Viene individuato come organo competente per la gestione delle infrazioni dei singoli alunni il Consiglio di Classe. I provvedimenti disciplinari da adottare nei confronti dell'alunno che ha commesso un'infrazione alla Policy, dopo aver tenuto conto sia dell'età dell'alunno che della gravità dell'infrazione commessa, saranno i seguenti:

- richiamo verbale;
- nota informativa sul diario ai genitori;
- 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.

1.5. Monitoraggio dell'implementazione della Policy e suo aggiornamento

Nel mese di maggio di ogni anno scolastico la commissione Bullismo e Cyberbullismo (formata da referente, animatore digitale, referente PTOF, più un referente per ogni plesso della scuola primaria e secondaria di primo grado) si riunirà con l'obiettivo di esaminare i casi problematici riscontrati durante l'anno e la loro gestione, in tale occasione valuterà la necessità o meno di modificare o implementare la Policy.

1.6. Integrazione della Policy con regolamenti esistenti

Il presente documento si integra pienamente per obiettivi e contenuti con il PTOF e con i regolamenti già in vigore nell'Istituto Comprensivo quali:

- 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

Per ciò che concerne Il curricolo sulle competenze digitali si fa riferimento al modello europeo della certificazione delle competenze.

2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica e sull'uso consapevole di Internet e delle tecnologia digitali

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 dal Collegio Docenti;

All'inizio di ogni anno scolastico la commissione Bullismo e Cyberbullismo, valutato a quali progetti/iniziative aderire e quali attività svolgere durante l'anno in corso, presenterà le sue proposte al Collegio Docenti per l'approvazione e la condivisione.
Nel corso dell'anno scolastico 2016/2017, 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 di bullismo, anche informatico*" (Legge 107/2015, art. 1, c. 7, l), il nostro Istituto ha aderito al progetto "Generazioni Connesse", coordinato dal MIUR. Tale progetto prevede lo svolgimento di un Piano d'Azione che ha diversi ambiti di sviluppo, tra cui la formazione docente.

2.3. Sensibilizzazione delle famiglie

Sarà creato sul sito della scuola un'area dedicata alla sicurezza in rete nella quale saranno inseriti materiali in formato PDF e link di video che illustrano i principali rischi che può incontrare un bambino o un adolescente attraverso la navigazione in rete. Tali materiali affronteranno tematiche quali il cyberbullismo, il sexting e l'adescamento.
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 per 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 ad Internet

L'accesso ad internet è possibile in tutti i plessi dell'Istituto (scuola secondaria di primo grado e scuola primaria)
Nei plessi delle scuole primarie e secondaria di primo grado l'accesso a internet è possibile in ogni aula dotata di LIM e nei laboratori di informatica.

3.2. Gestione accessi (password)

Nei computer presenti nelle aule e nei laboratori sono previsti due profili di accesso con password relative:

- amministratore;
- docente;

È possibile effettuare installazioni e aggiornamenti di software solo tramite la password di amministratore, fornita al personale di assistenza tecnica e all'Animatore Digitale.

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. La posta elettronica è protetta da antivirus e da antispam.

3.4 Protezione dei dati personali

Il trattamento dei dati personali riguarda unicamente le finalità istituzionali della scuola per le quali vengono raccolti solo i dati strettamente necessari. Essi saranno trattati con o senza l'ausilio di strumenti elettronici e comunque automatizzati secondo le modalità e le cautele previste dall'art. 13 del D. Lgs 196/2003 e conservati per il tempo necessario all'espletamento delle attività amministrative e istituzionali.

4. Strumentazione personale

4.1. Studenti

Nell'Istituto non è consentito agli alunni di portare a scuola i telefoni cellulari. 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.

4.2. Docenti

Durante le ore di lezione è consentito ai docenti l'uso di dispositivi elettronici personali, unicamente a scopo didattico e a integrazione dei dispositivi scolastici disponibili (computer di classe tablet della scuola). 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. Personale della scuola

Durante l'orario di servizio al restante personale scolastico l'uso del cellulare è consentito per comunicazioni personali urgenti, previa richiesta autorizzazione alla Dirigente Scolastica. 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

Rischi

Gli insegnanti, per la natura stessa del loro lavoro, devono in molti casi fungere da "torre di avvistamento", avamposto privilegiato delle problematiche e dei rischi che bambini e adolescenti possono trovarsi ad affrontare ogni giorno.
Responsabilità degli insegnanti è, dunque, 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 e non, 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;
- **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;

I rischi che gli alunni possono correre a scuola derivano da un uso non corretto dei dispositivi elettronici, in particolare di quelli personali.

Azioni

Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli studenti 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, attraverso la creazione di un'apposita area sul sito della scuola dedicata alla sicurezza in rete;
- Incontri con polizia Postale
- Sportello ascolto
- 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);
- Attento monitoraggio da parte del personale docente affinché il presente regolamento venga rispettato;
- Tempestivo intervento tramite opportuna sanzione qualora il regolamento venga disatteso;

5.2. Rilevazione

Cosa segnalare e come segnalare

La scuola ha il dovere di monitorare le attività svolte al suo interno attraverso i dispositivi digitali, ogni docente è invitato quindi a segnalare la presenza su un dispositivo in dotazione alla scuola dei seguenti contenuti:

- 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.

Il personale della scuola, 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 più approfondite indagini; 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 stampare i messaggi per fornire le eventuali prove degli 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 e, 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;
- Una nota disciplinare tramite registro elettronico;
- Una convocazione formale dei genitori degli alunni, tramite segreteria;
- Una convocazione delle famiglie da parte del Dirigente Scolastico;

Per i fatti più gravi la scuola si rivolgerà direttamente agli organi di polizia competenti.
La scuola non può intervenire su ciò che gli alunni svolgono fuori da essa con strumenti digitali ma qualora il docente venisse a conoscenza di eventuali atti scorretti come la condivisione di foto non autorizzate o l'insulto da parte di un alunno ad un compagno sul gruppo classe di WhatsApp (la creazione dei gruppi classe su WhatsApp è oggi una pratica molto diffusa) dovrà tempestivamente invitare le famiglie degli alunni coinvolti ad un attento monitoraggio delle attività svolte dai propri figli in rete.

5.3 Gestione dei casi

Per quanto riguarda la gestione dei casi il nostro Istituto ha individuato una figura referente.
La segnalazione del caso dovrà quindi essere fatta dal singolo docente, tramite modulo allegato al presente documento (allegato 1), alla referente, la quale si occuperà di raccogliere tutte le informazioni possibili e di segnalare l'accaduto alla Dirigente. Sarà poi la Dirigente a valutare se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali o se il caso vada gestito all'interno della scuola con il
coinvolgimento del Consiglio di Classe e delle famiglie degli alunni coinvolti.
La commissione bullismo e cyberbullismo si occuperà di tenere un *Diario di bordo* (allegato 2) per monitorare la situazione all'interno dell'Istituto e poter pianificare specifiche azioni preventive.

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

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:

- **È pervasivo**: il bullo può raggiungere la sua vittima in qualsiasi momento e in qualunque luogo;
- **È un fenomeno persistente**: il materiale messo online vi può rimanere per molto tempo;
- **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 (denunciato dalla vittima stessa, da persone vicino alla vittima o scoperto da un docente) si procederà nel modo seguente.

- Il docente venuto a conoscenza del fatto dovrà:
  - ❖ Informare tempestivamente la referente tramite modulo;
  - ❖ Informare tempestivamente il Consiglio di Classe dell'alunno oggetto di cyberbullismo;
  - ❖ Informare i genitori dell'alunno oggetto di cyberbullismo, offrendo loro la possibilità di avere il supporto della psicologa della scuola per affrontare al meglio la situazione;
- La referente, in collaborazione con il CdC raccoglierà tutte le informazioni possibili;
- Il CdC:
  - ❖ valuterà, a seconda della gravità del caso, come sanzionare il/i responsabili (qualora sia stato possibile individuarli);
- La Dirigente valuterà se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali;

Casi di sexting

Con il termine *sexting* si intende l'invio e/o la ricezione e/o la condivisione di testi, video o immagini sessualmente esplicite tramite cellulare o tramite internet.
Qualora ci si trovi di fronte ad un caso di sexting (denunciato dalla vittima stessa, da persone vicino alla vittima o scoperto da un docente) si procederà in maniera analoga ai casi di cyberbullismo.

Casi di adescamento online o *grooming*

Le tecnologie digitali consentono ai giovani di ampliare la propria rete di amicizie in modo quasi smisurato: non di rado gli adolescenti "concedono" la loro amicizia non solo a persone che conoscono direttamente, ma anche ad "amici di amici". Questo li espone a rischi notevoli, come quello di dare accesso a sconosciuti al loro mondo online e quindi a informazioni personali.
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). In un primo tempo, l'adulto, spesso mentendo sulla propria identità e sulla propria età, mostra particolare interesse nei confronti del/la bambina/a o dell'adolescente, cercando di conquistarne la fiducia. Solo in un secondo tempo, cerca di entrare sempre più nell'intimità del bambino fino a introdurre argomenti intimi e attinenti alla sfera sessuale.
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., si procederà nel modo seguente.

- Il docente venuto a conoscenza del fatto dovrà:
  - ❖ Informare tempestivamente la referente tramite modulo;
  - ❖ Informare tempestivamente il Consiglio di Classe dell'alunno oggetto di adescamento;
  - ❖ Informare i genitori dell'alunno oggetto di adescamento;
- La referente in collaborazione con il CdC raccoglierà tutte le informazioni possibili;
- La Dirigente valuterà se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali;

IL DIRIGENTE SCOLASTICO
Dott.ssa Mariantonia PUNTILLO

Allegato 1

MODULO PER LA SEGNALAZIONE

(Il presente modulo va compilato dal docente che raccoglie la segnalazione con la collaborazione dello studente)

- Episodio di:
  - Bullismo
  - Cyberbullismo
  - Sexting
  - Grooming
- Alunni coinvolti:
  - Vittima/e _____
  - Responsabile/i _____
- Quando? _____
- Dove? _____
- Descrizione del fatto:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Data _____ Il docente

_____

Allegato 2

Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi

Scuola_____Anno Scolastico_____

N°	Data	ora	Episodio (riassunto)	Azioni intraprese		Insegnante con cui l'alunno/a si è confidato	Firma
				Cosa?	Da chi?		