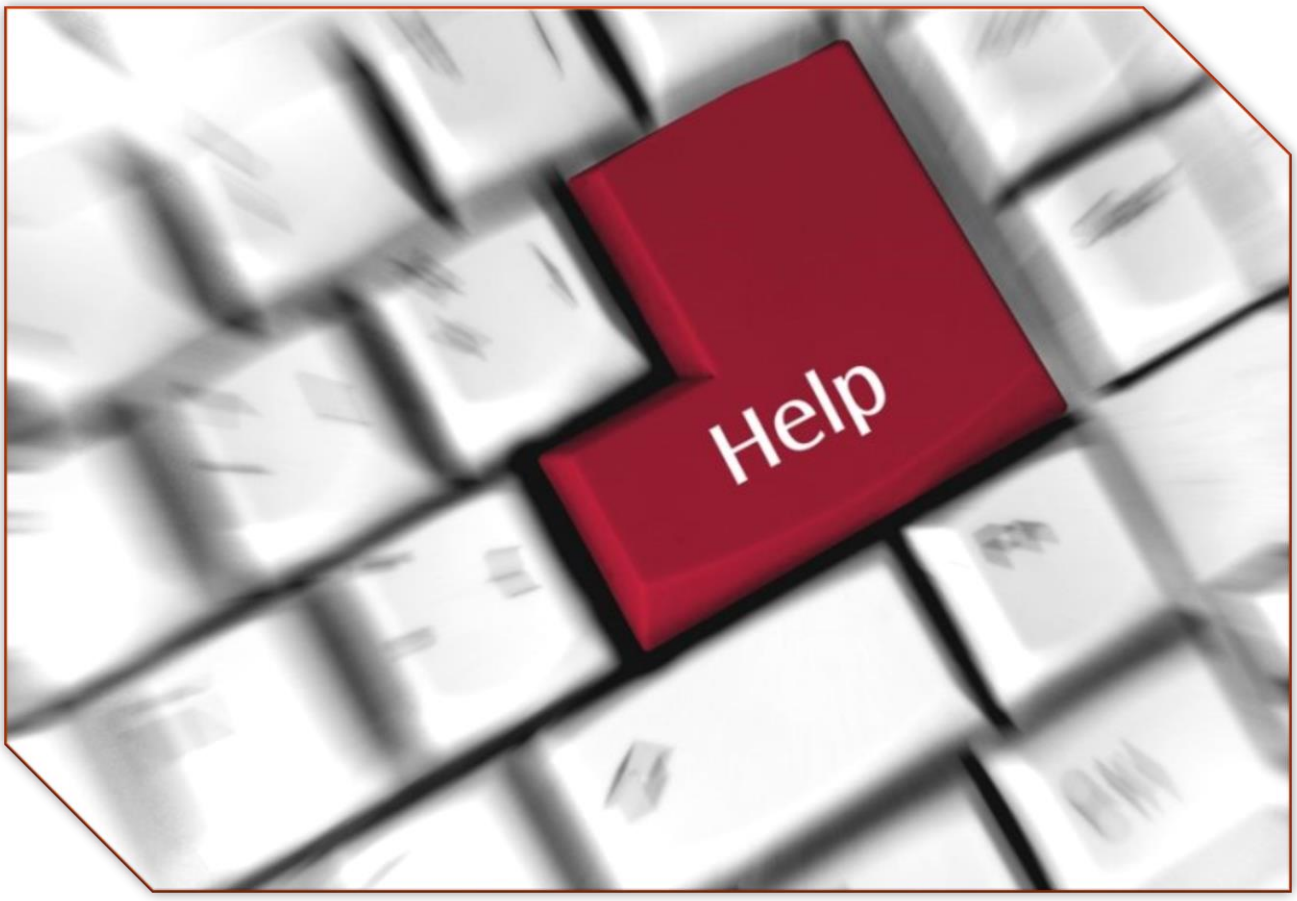
IV CIRCOLO DIDATTICO "CAROLINA SENATORE"
Ambito n.25 – Cod.SAEE165005
Scafati (SA) 84018 Via Martiri D'Ungheria
Traversa F.lli Bandiera
Parco Sereno Tel./Fax 081.8561645 – Tel.081.8568437 – 081.8630999
e-mail: saee165005@istruzione.it http://www.quartocircoloscafati.gov.it
e-mail: saee165005@pecistruzione.it – Codice Fiscale 94014660651

E- SAFETY POLICY

a.s.2017/18



Prot. N. 1968/7.5

E- Safety Policy- IV Circolo Scafati

1. INTRODUZIONE

Internet è un'inestimabile risorsa per l'informazione e la formazione personale, offre molteplici opportunità per comunicare, documentare, far ricerca, pubblicare, condividere esperienze ed attività.

In questo ambito risulta necessario acquisire e padroneggiare le competenze di cittadinanza digitale che oggi più che mai sono imprescindibili, se si considera che le nuove generazioni vivono "immerse" negli spazi di virtualità offerti dalla Rete che, troppo spesso, coincide con la dimensione del reale. Pertanto, occorre dare alle alunne e agli alunni gli strumenti per una piena consapevolezza dei rischi delle proprie interazioni in Rete e nei diversi media, per comprendere i meccanismi di produzione e circolazione delle informazioni, con particolare attenzione ai temi dell'identità e della privacy, alle caratteristiche specifiche della socialità in Rete e alla promozione della Rete come bene digitale comune.

Obiettivo primario è, pertanto, fornire strumenti di educazione civica digitale per prevenire situazioni di disagio online, evitare fenomeni di bullismo, forme di incitamento all'odio e di osservazione passiva ai vari comportamenti discriminatori, migliorare la comprensione e la consapevolezza dei diritti e della responsabilità in Rete.

1. a SCOPO DELLA POLICY

Lo scopo dell'E-Safety Policy d' Istituto è l'elaborazione di linee guida di un proprio codice di comportamento per la prevenzione, la gestione dei casi di (cyber)bullismo e di un regolamento di sicurezza informatica per favorire un uso corretto e responsabile delle tecnologie di comunicazione di Internet a scopo didattico, personale e ricreativo.

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

1. b RUOLI E RESPONSABILITA'

Dirigente Scolastico:

- ha un ruolo di intermediario tra l'istituzione scolastica e gli enti esterni del territorio preposti al contrasto del cyberbullismo;
- è responsabile della presentazione del suddetto regolamento al Collegio dei docenti e al Consiglio d'Istituto, al fine di valutarne l'efficacia e indirizzarne l'attuazione;
- assicura al personale una formazione adeguata.

Al dirigente vanno comunicate tempestivamente le informazioni relative ad azioni di mancato rispetto del regolamento.

Personale docente, in particolare i Coordinatori di classe:

- conosce le buone pratiche sulla sicurezza informatica;
- prende visione e sottoscrive l'e- policy d'Istituto;
- accompagna gli alunni nella navigazione in Rete, promuovendo comportamenti corretti, sicuri e responsabili nell'uso della Ret;
- inserisce tematiche relative alla sicurezza online nel programma di studi;
- indirizza la navigazione delle alunne e degli alunni verso siti sicuri;
- osserva le dinamiche relazionali che si sviluppano in classe e i cambiamenti di comportamento delle alunne e degli alunni;
- collabora con la classe, i colleghi- docenti, la famiglia e gli stakeholders coinvolti;
- informa i genitori circa la possibilità di attivare forme di controllo parentale della navigazione e sensibilizza sulla necessità di monitorare l'esperienza online dei propri figli;
- convoca, in caso di comportamenti violanti le buone norme di convivenza civile, i genitori dei soggetti interessati per condividere informazioni e concordare adeguate strategie e azioni educative;
- segnala tempestivamente al Dirigente scolastico o al Gruppo di Progetto ogni caso, anche solo sospetto, qualora il comportamento rappresenti un vero e proprio illecito, compilando l'apposito modulo di segnalazione e il diario di bordo delle situazioni gestite;
- verifica gli esiti delle azioni didattico-educative intraprese per rimodulare gli interventi.

Gruppo di Progetto:

- elabora strumenti conoscitivi del fenomeno;
- cura la redazione e la revisione annuale dell'e-policy e ne assicura la massima diffusione tra tutti i componenti della comunità scolastica;
- fa proposte operative di miglioramento;
- riferisce al Dirigente Scolastico casi/situazioni problema di particolare rilievo che necessitano di interventi;
- tiene un registro di incidenti per la sicurezza online;
- coordina con le autorità locali e le agenzie competenti.

Animatore e team digitale:

- promuove iniziative di formazione interna negli ambiti di sviluppo della formazione digitale, fornisce consulenza al personale in relazione ai rischi on-line e alle misure di prevenzione degli stessi;
- coinvolge la comunità scolastica nella partecipazione ad attività e progetti attinenti la "scuola digitale",
- contribuisce alla diffusione dell'e policy e del materiale informativo attraverso la pubblicazione sul sito istituzionale;
- realizza una pagina facebook per favorire la massima circolazione delle informazioni;
- gestisce l'assistenza tecnico- informativa per definire le misure di sicurezza informatica più opportune.

Direttore dei servizi generali e amministrativi:

- assicura, nei limiti delle risorse finanziare disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante e sicura;
- garantisce il funzionamento dei diversi canali di comunicazione della scuola(circolari, sito web,…) .

Personale ATA:

- prende visione e sottoscrive l'e- policy d'Istituto;
- mantiene tutte le comunicazioni digitali con i genitori/tutori a livello professionale;
- segnala qualsiasi abuso, anche sospetto, al Dirigente Scolastico, al Gruppo di Progetto e all'Animatore Digitale per le necessarie azioni/sanzioni.

Genitori:

- sostengono le linee di condotta della scuola adottate per l'utilizzo delle TIC;
- comunicano, collaborano e concordano con i docenti linee di intervento di carattere educativo in materia di prevenzione e di gestione dell'uso delle tecnologie digitali;
- aiutano i propri figli a riconoscere le risorse del web e sono esempio di interazioni costruttive;
- monitorano attentamente e sistematicamente i propri figli nella navigazione sul web;
- utilizzano dispositivi di controllo parentale sul pc;
- partecipano a corsi di formazione/convegni organizzati dalla scuola relative alla sicurezza digitale.

Alunne/alunni

- non utilizzano dispositivi digitali personali durante le attività didattiche;
- assumono atteggiamenti responsabili nell'utilizzo delle tecnologie digitali;
- segnalano ai docenti e/o ai genitori ogni abuso o uso improprio della Rete.

1. c CONDIVISIONE E COMUNICAZIONE DELLA POLICY ALL'INTERA COMUNITA' SCOLASTICA

1. d Azioni e iniziative:

- presentazione della policy al Collegio dei Docenti e al Consiglio di Istituto;
- pubblicazione dell'e-policy sul sito della scuola;
- confronto collegiale, su base annuale, circa la necessità di apportare modifiche e miglioramenti alla policy attuale;

- elaborazione di protocolli di intervento condivisi;
- inserimento, nel diario degli alunni, di sintesi del documento della policy e dei comportamenti di tutela da attivare;
- organizzazione di incontri/seminari, anche con esperti esterni, di informazione e sensibilizzazione rivolti a tutte le componenti della Comunità Scolastica.

1. e GESTIONE DELLE INFRAZIONI DELLA POLICY:

- rilevazioni delle infrazioni alla Policy da parte dei docenti/personale ATA / genitori nell'esercizio delle proprie funzioni;
- obbligo della comunicazione tempestiva di casi /situazioni problema di particolare rilevanza al Dirigente Didattico per gli adempimenti del caso;
- attivazione delle procedure previste dal Regolamento di Istituto per le infrazioni che violano le norme previste dal Regolamento stesso.

1. f MONITORAGGIO DELL'IMPLEMENTAZIONE DELLA POLICY E SUO AGGIORNAMENTO

- confronto collegiale annuale su eventuali proposte di modifica e miglioramenti della policy vigente da parte di tutte le componenti della Comunità Scolastica.

1. g INTEGRAZIONE DELLA POLICY CON REGOLAMENTI ESISTENTI:

- la presente Policy è allegata al Regolamento di Istituto.

2. FORMAZIONE E CURRICOLO

2. a Curricolo sulle competenze digitali per gli studenti

La scuola incrementa l'uso delle tecnologie informatiche, guida e sostiene le alunne e gli alunni nell'acquisizione delle norme comportamentali e delle procedure per l'utilizzo delle TIC al fine di promuovere le competenze di cittadinanza digitale. L'accesso agli strumenti digitali va, pertanto, inserito nell'esperienza di apprendimento come metodologia didattica diffusa.
Nell'ambito del PSND è previsto un programma di educazione alla sicurezza online come parte del curriculum scolastico.
L' alunno/a

- conosce procedure di coding e partecipa a laboratori nella settimana del codice;
- utilizza strumenti informatici in situazioni significative di gioco e di relazione con gli altri;
- usa mezzi di comunicazione ed è in grado di farne un impiego adeguato a seconda delle diverse situazioni.

1. b Formazione dei docenti sull'utilizzo e l'integrazione delle tic nella didattica

Il Piano Nazionale di Formazione sulle Competenze Informatiche e Tecnologiche del Personale della scuola, avviato con la circolare 55, ha il merito di avere individuato anche nel nostro Istituto tre delle modalità, considerandole come strategiche:

- allargare il numero dei docenti con competenze da utenti di informatica (con un corso settimanale di formazione su due livelli);
- formare un esperto di tecnologia educativa (animatore digitale);
- costituire un nucleo di docenti/tecnici esperti sugli aspetti strettamente tecnici e tecnologici delle reti informatiche capaci di mantenere dall'interno i sistemi informatici della scuola (team digitale).

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

- Formazione di alunni e docenti delle classi terminali del Circolo relativamente all'utilizzo consapevole e sicuro di Internet e delle tecnologie.

2 d Sensibilizzazione delle famiglie.

- Sensibilizzazione delle famiglie all'uso consapevole di Internet da parte dei minori attraverso incontri-dibattiti con la partecipazione di esperti del settore.

3 GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA

3 a Accesso ad Internet: filtri, antivirus e sulla navigazione

- La scuola ha installato su pc e notebook filtri di protezione anche se gli alunni non accedono alla navigazione senza la sorveglianza dei docenti.

3 b Gestione accessi (password, backup, ecc.)

- Tutti i pc presenti a scuola hanno accesso libero.

3 c E-mail

- Ogni docente possiede una propria e-mail istituzionale e taluni anche mail private.

3 d Blog e sito web della scuola

L' Istituto ha un sito web; questo spazio è cresciuto e si è evoluto grazie alla partecipazione di tutte le componenti della Scuola (Dirigente Scolastico, docenti, personale di Segreteria). Il sito www.quartocircolo.gov.it per la sua fruibilità, riceve numerosissime visite, la sua presenza sul web permette sicuramente una grande visibilità ed una efficacia pubblicizzazione del nostro Istituto.

Le finalità perseguite hanno lo scopo di:

- presentare le attività programmate;

- offrire occasioni di aggiornamento ai docenti attraverso materiali e documenti;

- condividere le informazioni;

- stimolare la partecipazione e la condivisione di esperienze;

- coinvolgere gli alunni, i genitori e gli enti;

- offrire all'utenza occasione di partecipazione.

Tutti i contenuti didattici sono pubblicati direttamente e sotto supervisione dell'animatore digitale che ne valuta l'adeguatezza e la sicurezza.

3 e Social network

- Il IV Circolo Didattico di Scafati ha una pagina sul social facebook dove vengono pubblicate notizie relative alle varie iniziative didattiche.

3 f Protezione dei dati personali

- Il personale scolastico è incaricato del trattamento dei dati personali (alunni, genitori,…) nei limiti della propria funzione.
  I dati personali degli alunni in forma digitale, presenti sul portale ARGO, sono gestiti a norma di legge e l'accesso è consentito unicamente con password e username fornite ai docenti personalmente dall'Amministrazione. Le fotografie e i video da pubblicare sul sito che includono alunne /alunni saranno selezionate con cura e non permetteranno ai singoli di essere identificati se non è stata richiesta specifica autorizzazione ai genitori.

4. STRUMENTAZIONE PERSONALE

4 a - Per gli studenti: gestione degli strumenti personali- cellulare, tablet ecc.

- Non è consentito a scuola l'uso di dispositivi personali.

4 b - Per i docenti: gestione degli strumenti personali- cellulare, tablet ecc.

- Durante le ore di lezione non è consentito l'uso del cellulare; i docenti usano sporadicamente device personali per uso didattico/gestionale (registro elettronico), in caso di cattivo funzionamento della rete.

4 c Per il personale della scuola: gestione degli strumenti personali- cellulare, tablet ecc.

- Il personale utilizza in casi eccezionali i device personali.

5 PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

5 a Prevenzione

- **Azioni**:
  - informare e formare i docenti, il personale ATA, i genitori e gli studenti sull'uso corretto delle tecnologie digitali;
  - riconoscere il Dirigente Scolastico come titolare del trattamento dei dati personali secondo la Legge sulla privacy (art. 41 f del Dlgs 196/2003);
  - promuovere la partecipazione a progetti e a concorsi;
  - organizzare corsi di formazione, incontri, seminari per docenti, genitori, alunni;
  - scaricare o installare solo software autorizzati;
  - condividere e /o pubblicare materiali didattici solo con il permesso di ciascun utente coinvolto, sempre nel rispetto del presente regolamento;
  - informare i genitori circa l'attivazione del controllo parentale della navigazione;
  - prevedere interventi mirati sul gruppo-classe;
  - includere nel curricolo tematiche quali la legalità, la diversità di genere, l'inclusività.

- **Rilevazione:**
  - segnalare abusi solo se i contenuti e i comportamenti risultano palesemente impropri ed illeciti;
  - rilevare casi tra gli alunni attraverso azioni di monitoraggio in forma anonima;
  - utilizzare la modulistica messa a disposizione sul sito www.generazioniconnesse.it sia per la registrazione che per la gestione dei casi (allegato n° 1 -2).

Procedure operative per la gestione delle infrazioni alla Policy

Studenti:

INFRAZIONI	EVENTUALI SANZIONI/PROCEDURE
Uso non autorizzato del telefono cellulare o di altre tecnologie durante le lezioni.	Rimozione del telefono e consegna ai genitori. Richiamo scritto con annotazione sul diario. Convocazione dei genitori da parte del Consiglio di Classe. Convocazione dei genitori da parte del Dirigente Scolastico.

Personale scolastico:

INFRAZIONI	EVENTUALI SANZIONI/ PROCEDURE
Uso di Internet per attività personali non professionali	

Utilizzo di supporti di memorizzazione dati	Richiamo verbale
Comportamenti sul web lesivi della professionalità dei docenti e della scuola	Avvertimento
Violazione del copyright o della licenza per installare software	
Diffusione non autorizzata di materiali	Rapporto alle autorità competenti
con infrazioni delle condizioni previste dalla legge sulla protezione dei dati	
Gravi danni intenzionali all'hardware o software del pc	
Uso improprio di primo livello di sicurezza di dati (password…)	
Creazione, accesso e diffusione materiali offensivi, osceni, razzisti, omofobici, violenti	

Procedure operative per la protezione dei dati personali

Si fa riferimento a tutto quanto previsto dal *Decreto legislativo30 giugno 2003, n. 196* (c.d. Codice della Privacy). In questa prospettiva è richiesto alle famiglie di firmare, per ogni evento o manifestazione, un'autorizzazione scritta per consentire l'uso didattico di immagini e video delle/dei minori, che non violino la legge.

Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni

La rilevazione dei casi è compito di tutta la comunità educante; i docenti, in particolare sono chiamati ad attivare atteggiamenti di sensibilizzazione dei rischi, di accoglienza e di ascolto delle situazioni problematiche. Si prevedono azioni di monitoraggio in forma anonima.

Procedure operative per la gestione dei casi

La gestione dei casi rilevati va differenziata in relazione alla loro gravità; è richiesta la comunicazione al Dirigente Scolastico, la condivisione a livello di Consiglio di Classe/ Interclasse degli episodi rilevati, la convocazione dei genitori per riflettere ed elaborare insieme strategie didattico/educative, tenere tracce delle azioni intraprese, contattare il servizio helpline messo a disposizione da Generazioni Connesse.

Nei casi più gravi e in ogni ipotesi di reato, il Dirigente Scolastico valuterà l'opportunità di procedere alla segnalazione alle autorità competenti.

Il presente Regolamento è stato approvato in data 23/04/2018 dal Collegio Docenti del IV Circolo "C. Senatore", e dal Consiglio d'Istituto in data 24/04/2018.

Scafati 24/04/2018

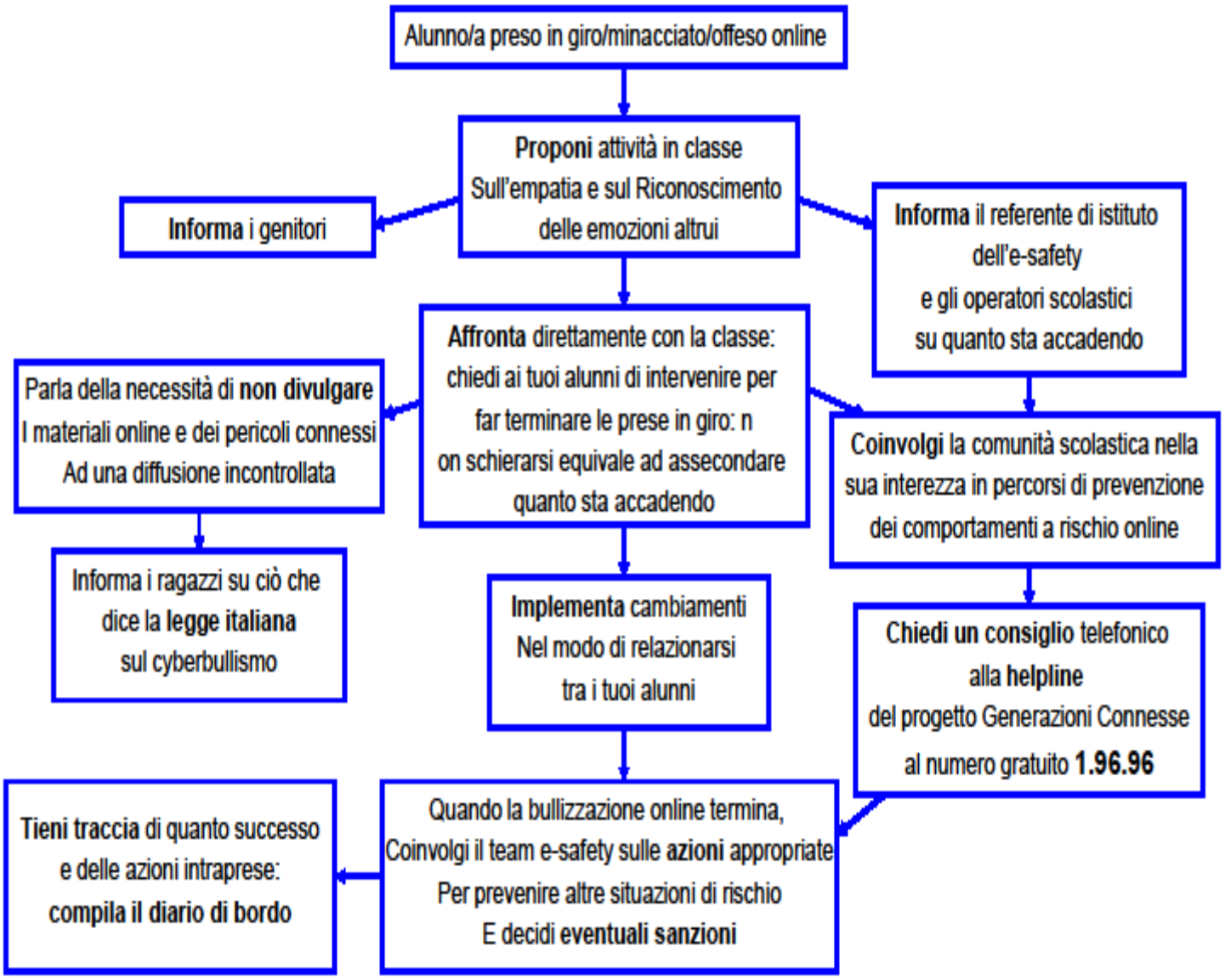
Il Dirigente Scolastico
Prof.ssa Ester Senatore
(Il documento è firmato digitalmente ai sensi del D. Lgs. 82/2005, s .m.i. e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa)

CO-FINANZIATO DALLA COMMISSIONE EUROPEA

Sicurezza in rete - Schema per la scuola

Cosa fare in caso di... cyberbullismo?

Generazioni Connesse
SAFER INTERNET CENTRE



Polizia di Stato

Save the Children

E.D.I.

CO-FINANZIATO DALLA COMMISSIONE EUROPEA

Sicurezza in rete – formazione insegnanti

Modulo di segnalazione casi

Generazioni Connesse SAFER INTERNET CENTRE

Classe _____ **Istituto (se plesso)** _____			
Data _____	*Ora* _____	*Luogo* _____	*riferito da?* _____
Cosa è successo?			
Responsabile/i		Vittima/e	
			Firma _____
Aggiornamento 1			
Aggiornamento 2			
Aggiornamento 3			

Polizia di Stato

TELEFONO AZZURRO

Autorità Garante per l'Infanzia e l'Adolescenza

Save the Children

E.D.I.

Co-financed by the European Union
Connecting Europe Facility

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?		

PROGETTO GENERAZIONI CONNESSE

MODULO PER LA SEGNALAZIONE DI CASI

Nome di chi compila la segnalazione: Ruolo:

Data: Scuola:

Descrizione dell'episodio o del problema	
Soggetti coinvolti	Vittima/e: Classe: 1. 2. 3. Bullo/i: Classe: 1. 2. 3.
Chi ha riferito dell'episodio?	- La vittima - Un compagno della vittima, nome: - Genitore, nome: - Insegnante, nome: - Altri, specificare:
Atteggiamento del gruppo	Da quanti compagni è sostenuto il bullo? Quanti compagni supportano la vittima o potrebbero farlo?
Gli insegnanti sono intervenuti in qualche modo ?	
La famiglia o altri adulti hanno cercato di intervenire ?	
Chi è stato informato della situazione?	☐ coordinatore di classe data: ☐ consiglio di classe data: ☐ dirigente scolastico data: ☐ la famiglia della vittima/e data: ☐ la famiglia del bullo/i data: ☐ le forze dell'ordine data: ☐ altro, specificare:

MODULO PER IL FOLLOW-UP DEI CASI

	AZIONI INTRAPRESE	La situazione è
Aggiornamento 1		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 2		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 3		☐ migliorata ☐ invariata ☐ peggiorata Come:

Modello per la segnalazione/reclamo in materia di cyberbullismo

(ai sensi dell'art. 2, comma 2, legge 29 maggio 2017, n. 71, Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo)

Al Garante per la protezione dei dati personali
Inviare all'indirizzo e-mail: cyberbullismo@gpdp.it

Il/La sottoscritto/a _____([1]), nato/a a _____, il _____, residente a _____, via/p.za _____, tel. _____, e-mail/PEC _____ *[inserire recapiti ai quale si può essere contattati e selezionare, di seguito, l'opzione pertinente]*,

- ☐ minore ultraquattordicenne,

  ovvero

- ☐ in qualità di esercente la responsabilità genitoriale sul minore _____, nato a _____ il _____.

SEGNALA

1. di essere stato/a vittima ovvero che il minore sul quale esercita la responsabilità genitoriale è stato vittima di cyberbullismo [*eliminare la locuzione che non interessa*]. In particolare, i comportamenti posti in essere, **realizzati per via telematica** e di seguito sinteticamente descritti, consistono in [*selezionare la/e fattispecie rilevanti*]

- ☐ pressione
- ☐ aggressione
- ☐ molestia
- ☐ ricatto
- ☐ ingiuria
- ☐ denigrazione
- ☐ diffamazione
- ☐ furto d'identità
- ☐ alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati

[1] Avvertenza: la segnalazione o il reclamo può essere presentata direttamente anche da minori d'età ultraquattordicenni ovvero da chi esercita la responsabilità genitoriale. Pertanto si prega il segnalante/reclamante di fornire le pertinenti informazioni.

ovvero

- ☐ diffusione di contenuti *on line* aventi ad oggetto il minore ovvero uno o più componenti della famiglia del minore *[rimuovere l'informazione non rilevante]* allo scopo intenzionale e predominante di isolare il minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo.

2. che la diffusione di contenuti lesivi dell'interessato/a è avvenuta [*selezionare la casella pertinente*]:

- ☐ sul sito internet _____ all'indirizzo web [*necessario indicare URL*]
  _____
- ☐ *social media* [*necessario inserire individuazione univoca*]
  _____
- ☐ altro [*necessario specificare*]
  _____

3. Allega i seguenti documenti (ad es. immagini, video, *screenshot*, etc.):

1) _____
2) _____
3) _____

4. Inserire una sintetica descrizione dei fatti:

_____
_____
_____
_____
_____
_____

Tanto premesso, [*selezionare l'opzione pertinente*]

- ☐ considerato che il gestore del sito internet o del *social media* al quale è stata presentata l'istanza allegata per l'oscuramento, la rimozione o il blocco dei dati personali diffusi in internet

non ha comunicato entro 24 ore di avere assunto l'incarico di provvedere all'oscuramento, alla rimozione o al blocco richiesto, né vi ha provveduto entro quarantotto ore *[allegare la pertinente documentazione]*;

- considerato che non è stato in grado di presentare un'istanza per l'oscuramento, la rimozione o il blocco dei dati personali diffusi in internet al gestore del sito internet o del *social media* non essendo possibile identificare il titolare del trattamento o il gestore del sito internet o del *social media*,

RICHIEDE AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

di disporre, ai sensi degli articoli 2, comma 2, l. n. 71/2017 nonché 143 e 144, d.lgs. n. 196/2003, il blocco/divieto della diffusione dei dati personali sopra descritti.

Il/La sottoscritto/a dichiara inoltre di *[selezionare la casella pertinente]:*

- aver presentato denuncia/querela per i fatti sopra descritti presso _____;
- non aver presentato denuncia/querela per i fatti sopra descritti.

Luogo, data

Nome e cognome

Informativa ai sensi dell'art. 13 del Codice in materia di protezione dei dati personali

Il Garante per la protezione dei dati personali tratterà i dati personali trasmessi, con modalità elettroniche e su supporti cartacei, per lo svolgimento dei compiti istituzionali nell'ambito del contrasto del fenomeno del cyberbullismo. Il loro conferimento è obbligatorio ed in assenza degli stessi la segnalazione/reclamo potrebbe non poter essere istruita. I dati personali potrebbero formare oggetto di comunicazione ai soggetti coinvolti nella trattamento dei dati personali oggetto

di segnalazione/reclamo (con particolare riferimento a gestori di siti internet e social media), all'Autorità giudiziaria o alle Forze di polizia ovvero ad altri soggetti cui debbano essere comunicati per dare adempimento ad obblighi di legge. Ciascun interessato ha diritto di accedere ai dati personali a sé riferiti e di esercitare gli altri diritti previsti dall'art. 7 del Codice.

COME PROTEGGERE VOSTRO FIGLIO DAI CYBERBULLI

Alcune semplici norme che si possono applicare per proteggere i vostri figli da tale fenomeno :

1. Educate al **rispetto** sia offline che online e promuovete comportamenti relazionali positivi in famiglia e fuori: i figli fanno riferimento, prima di tutto, ai **modelli che imparano dai genitori**.

2. **Partecipate** alle attività che vostro figlio/a svolge online, impegnatevi a conoscere non solo i contatti e i social a cui è iscritto/a, ma anche cosa fa, cosa lo/a interessa o lo appassiona online.

3. Stabilite insieme alcune semplici **regole di sicurezza** da seguire sempre. Per esempio, non accettare inviti o amicizie sui social network da parte di sconosciuti, informarvi se c'è qualcuno che lo/la inopportuna online, eccetera.

4. Prestate attenzione anche ai **piccoli cambiamenti** che avvengono nel suo comportamento e nei suoi atteggiamenti (non vuole più frequentare scuola o luoghi abitualmente frequentati, o si mostra preoccupato o in ansia ad ogni notifica che riceve sui social). Solo così potrete accorgervi se qualcosa lo/a turba.

5. **Dialogate**: mostrate a vostro figlio/a la vostra **disponibilità ad ascoltare**; create le condizioni affinché – qualora sorgano problemi – si senta libero/a di condividere le sue preoccupazioni, sicuro/a di trovare interlocutori attenti e **non giudicanti**.

6.**Pensare prima di postare**: Aiuta tuo figlio a riflettere prima di scrivere/postare/inoltrare: il Web non dimentica e spesso la diffusione è immediata e virale.