



Istituto Comprensivo “G. Carducci”

Via Sold. Zuffanti, 57 - 93016 Riesi (CL) - Tel.: 09341878250 - Codice Scuola: CLIC81700N

Cod. Fisc./P. Iva: 82002440855 - E-mail: clic81700n@istruzione.it

Sito Internet: www.icriesi.edu.it



E-Safety Policy

a.s. 2019/20

Approvato dal Collegio Docenti in data 15 ottobre 2019

Approvato dal Consiglio d'Istituto nella seduta del 23 ottobre 2019

INDICE RAGIONATO

1. Introduzione

- Scopo della Policy.
- Ruoli e Responsabilità (*che cosa ci si aspetta da tutti gli attori della Comunità Scolastica*):
 - a) Dirigente Scolastico
 - b) Animatore Digitale e Team dell'Innovazione come da PNSD
 - c) Direttore dei Servizi Generali e Amministrativi
 - d) Docenti
 - e) Alunni
 - f) Genitori
- Condivisione e comunicazione della Policy all'intera comunità scolastica.
- Gestione delle infrazioni alla Policy.
- Monitoraggio dell'implementazione della Policy e suo aggiornamento.
- Integrazione della Policy con Regolamenti esistenti.

2. Formazione e Curricolo

- Curricolo sulle competenze digitali per gli alunni.
- Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica.
- Sensibilizzazione delle famiglie.

3. Gestione dell'infrastruttura e della strumentazione ICT della scuola.

- Accesso ad internet: filtri antivirus e sulla navigazione.
- Gestione accessi (password, backup, ecc.).
- E-mail. Sito web della scuola
- Social network.
- Protezione dei dati personali.

4. Strumentazione personale

- Per gli alunni: gestione degli strumenti personali - cellulari, tablet ecc.
- Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc.
- Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc.

5. Prevenzione, rilevazione e gestione dei casi

➤ *Prevenzione*

- Rischi
- Azioni

➤ *Rilevazione*

- Che cosa segnalare
- Come segnalare: quali strumenti e a chi.
- Come gestire le segnalazioni.

6. Provvedimenti disciplinari in supporto all'azione educativa della Scuola

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

Allegati:

All. 1 Scheda di rilevazione delle segnalazioni

All. 2. Procedure operative per la gestione dei casi

All. 3. Modulo di richiesta per l'accesso ad Internet nella rete d'Istituto

All. 4. Consenso da parte dei Genitori per l'accesso ad Internet

All. 5. Consenso al trattamento dei dati personali

All.6. Liberatoria per la pubblicazione di fotografie e riprese video

1. INTRODUZIONE

Scopo della E-Safety Policy

Il presente documento segue le indicazioni delle LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrasto al bullismo e cyberbullismo (aprile 2015) elaborate dal Ministero dell'Istruzione, dell'Università e della Ricerca, al fine di perseguire i seguenti obiettivi:

- stabilire le misure di prevenzione e di gestione di situazioni problematiche relative all'uso di internet e delle tecnologie digitali;
- facilitare e promuovere l'utilizzo delle tecnologie nella didattica e negli ambienti scolastici;
- Lo scopo del presente documento, dunque, è quello di educare e sensibilizzare gli alunni, gli insegnanti, tutto il personale scolastico e i genitori all'uso sicuro e consapevole di Internet.

Gli utenti, siano essi docenti o alunni, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete, infatti, esiste la possibilità che durante il lavoro on-line ci si possa imbattere con materiale inadeguato, illegale e finanche pericoloso.

In particolare, la Policy viene redatta per regolare il comportamento interno ed esterno dell'intera comunità scolastica, adottando misure disciplinari da applicare su comportamenti scorretti, operando in stretto rapporto con l'Ufficio di Solidarietà sociale del Comune e con le Forze dell'Ordine del territorio al fine di individuare e attuare adeguate strategie di prevenzione.

Ruoli e Responsabilità (che cosa ci si aspetta da tutti gli attori della Comunità Scolastica).

- Dirigente Scolastico
- Animatore Digitale e Team dell'Innovazione come da PNSD
- Direttore dei Servizi Generali e Amministrativi
- Docenti
- Alunni
- Genitori

a) *Dirigente scolastico*

Il ruolo del Dirigente scolastico, nel promuovere l'uso delle tecnologie e di Internet, include i seguenti compiti:

- ✓ garantire la presentazione di questo documento all'attenzione del Consiglio di Istituto e al Collegio dei Docenti;
- ✓ garantire la sicurezza on-line dei membri della comunità scolastica;
- ✓ garantire che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle

differenze, un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della comunicazione (TIC);

- ✓ garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line.

b) Animatore Digitale e Team dell'Innovazione come daPNSD:

Il ruolo dell'Animatore Digitale e del Team dell'Innovazione include i seguenti compiti:

- **Formazione interna**
 - stimolare e organizzare attività di formazione interna alla scuola negli ambiti del PNSD favorendo l'animazione e la partecipazione di tutta la comunità scolastica.
- **Coinvolgimento della comunità scolastica**
 - favorire la partecipazione degli alunni in attività laboratoriali previste dal PNSD;
 - facilitare e implementare momenti di apertura della scuola alle famiglie e ad altri attori del territorio per la realizzazione di una cultura digitale condivisa.
- **Creazione di soluzioni innovative**
 - individuare soluzioni metodologiche e tecnologiche sostenibili da diffondere all'interno degli ambienti della scuola;
 - incrementare l'uso di particolari strumenti per la didattica di cui la scuola si è dotata;
 - stimolare l'adozione di metodologie innovative attraverso la socializzazione di buone pratiche;
 - divulgare informazione su innovazioni esistenti in altre scuole;
 - attivare attività laboratoriali di coding da estendere al maggior numero di alunni.

c) Direttore dei Servizi Generali e Amministrativi:

- ✓ assicurare, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione richiesti da cattivo funzionamento e/o danneggiamento della dotazione tecnologica dell'Istituto;
- ✓ controllare che le norme di sicurezza vengano rispettate;
- ✓ garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni
- ✓ per la notifica di documenti e informazioni del Dirigente Scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di Internet.

d) Docenti

Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali

e di Internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;

- sviluppare le competenze digitali degli alunni;
- illustrare ai propri alunni le norme di sicurezza nell' utilizzo del web e delle tecnologie digitali contenute nel presente documento;
- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo all'Animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e ai fini di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- segnalare al Gruppo di Lavoro, al Dirigente Scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di Internet, per l'adozione delle procedure previste dalle norme e dalla presente Policy.

e) *Alunni*

- ✓ ascoltare e seguire le indicazioni fornite dai docenti per un uso corretto e responsabile delle tecnologie digitali, attuando le regole di e-Safety per evitare situazioni di rischio;
- ✓ chiedere l'intervento dell'insegnante e/o dei genitori qualora insorgano difficoltà o dubbi nell'utilizzo degli strumenti digitali.

f) *Genitori*

- ❖ Sostenere la linea di condotta adottata dalla scuola nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;
- ❖ seguire i propri figli nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti;
- ❖ confrontarsi con i docenti per attivare linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati a causa di un uso non responsabile o pericoloso delle tecnologie digitali o di Internet;
- ❖ fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di Internet e di tutti i dispositivi usati.

Condivisione e comunicazione della Policy all'intera comunità scolastica.

Per evitare che l'adozione di questa “Policy” rappresenti un mero atto formale, l'Istituto si impegna a prendere spunto da essa come base di partenza per una serie di azioni e iniziative:

a) Per il corpo docente:

- promuovere discussioni collegiali sui contenuti, sulle pratiche indicate e su come inserire nel curriculum le tematiche di interesse della Policy;
- promuovere confronti collegiali circa la necessità di apportare modifiche e miglioramenti alla Policy vigente.

b) Per gli alunni:

- i docenti informeranno gli alunni sul fatto che l'uso di Internet di ogni dispositivo digitale saranno utilizzati solo con l'autorizzazione dell'insegnante;
- nel corso dell'anno, i docenti svilupperanno percorsi sull'utilizzo sicuro del digitale con
- specifico riferimento ai rischi della rete e alla lotta al cyberbullismo.

c) Per i 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 incontri informativi durante i quali si farà riferimento alla presente Policy;
- ❖ i genitori saranno sensibilizzati al fine di prestare la massima attenzione alle regole contenute nel presente documento affinché vengano rispettate dai propri figli anche in ambito domestico.

Gestione delle infrazioni alla Policy

a) Alunni

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali di Internet di cui si dispone per la didattica, in relazione alla fascia di età considerata, sono prevedibilmente le seguenti:

- un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;
- l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;
- la condivisione di immagini intime o troppo spinte;
- la comunicazione incauta e senza permesso con sconosciuti;
- il collegamento a siti web non indicati dai docenti.

Sono previsti da parte dei docenti i seguenti provvedimenti disciplinari:

- il richiamo verbale;
- il richiamo verbale con particolari conseguenze;
- il richiamo scritto con annotazione sul diario;
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente Scolastico.

b) Personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico incorra nell'utilizzo delle tecnologie digitali e di Internet sono diverse e alcune possono determinare, favorire o avere conseguenze di maggiore o minore rilievo:

- un 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;
- un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- un'eventuale diffusione delle password assegnate di cui possono approfittare terzi e una custodia non adeguata degli strumenti;
- una carente istruzione preventiva degli alunni sull'utilizzo corretto e responsabile delle tecnologie digitali e di Internet.

c) Genitori

Le situazioni familiari meno favorevoli ad un uso corretto e responsabile delle TIC possono essere:

- la convinzione che, se il proprio figlio usa il computer a casa, è al sicuro;
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone;
- un utilizzo condiviso con i propri figli del pc che può conservare in memoria
- materiali non idonei.

Monitoraggio dell'implementazione della Policy e suo aggiornamento.

La presente Policy sarà riesaminata annualmente e/o quando si verificano cambiamenti significativi anche in relazione a norme di *maggior valore* come regolamenti o Policy emanati dal MIUR ed eventuali leggi dello Stato.

Integrazione della Policy con Regolamenti esistenti.

Il presente documento si integra pienamente con obiettivi e contenuti dei seguenti documenti:

- ✓ PTOF e il Piano triennale per l'attuazione del PNSD;
- ✓ Regolamento interno d'istituto;
- ✓ Regolamento per l'utilizzo del laboratorio di informatica. Tale integrazione garantisce coerenza con il RAVe il PdM.

2. FORMAZIONE E CURRICOLO

Curricolo sulle competenze digitali per gli alunni.

La sicurezza in rete è un aspetto importante quando si lavora nella scuola.

La **competenza digitale** consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie sia per il lavoro che per il tempo libero. Essa è supportata da abilità di base nelle TIC: reperire, valutare, conservare, produrre, presentare e scambiare informazioni, nonché comunicare e partecipare a reti collaborative tramite Internet.

Competenze digitali:

- Far acquisire all'alunno la capacità di navigare in sicurezza.
- Favorire l'interiorizzazione dei comportamenti corretti da tenere durante la navigazione e su eventuali social network.
- Approfondire le tematiche relative alla netiquette (insieme di regole che disciplinano il comportamento di un utente in Internet).
- Imparare a comunicare ed interagire sui social network, in maniera idonea.
- Riconoscere i potenziali virus, file e mail infetti.

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

Durante il triennio 2016/2019 sono stati effettuati dei corsi di formazione sulle varie tematiche in oggetto e su diversi livelli di competenze.

Per questo nuovo anno scolastico, e per i successivi anni scolastici, relativi al prossimo triennio, si terranno in considerazione le istanze e i bisogni formativi dei docenti e si attiveranno corsi relativi alle tematiche maggiormente richieste, avendo come obiettivi:

1. la formazione dei docenti sull'utilizzo e sicuro di Internet e delle tecnologie digitali.
2. L'Implementazione delle competenze di ricerca sul web.
3. La formazione all'uso consapevole dei social network anche ai fini didattici.

In considerazione delle finalità già individuate nel Piano adottato dalla scuola si prevede nel

prossimo anno scolastico, anche alla luce della redazione della Policy e- Safety, di avviare degli incontri formativi con i docenti sul tema “*Sicurezza in rete*”.

Sensibilizzazione delle famiglie.

Saranno previsti incontri con le famiglie degli alunni per implementare le forme di vigilanza e le necessarie misure di restrizione funzionali per il corretto utilizzo dei contenuti reperibili in rete da parte dei minori.

3. GESTIONE DELL’ INFRASTRUTTURA E DELLA STRUMENTAZIONE ITC DELLA SCUOLA

Accesso a internet: filtri e antivirus.

Attualmente nella scuola è presente un’unica rete con connessione ADSL. È possibile connettersi a Internet nel laboratorio multimediale, nelle classi e nelle aree comuni della scuola. Nel laboratorio multimediale la connessione Internet è garantita da una rete LAN, invece, negli altri spazi, da collegamenti wireless. Nel laboratorio multimediale, vi è una postazione di lavoro per il docente e ventiquattro postazioni per gli alunni. L’accesso a Internet è schermato da filtri che consentono il collegamento solo a siti sicuri. Tutti i dispositivi in uso nella scuola sono muniti di antivirus. Il responsabile del laboratorio informatico, che coincide con l’animatore digitale, periodicamente provvede alla manutenzione del laboratorio informatico richiedendo, ove necessario, anche l’intervento di tecnici esterni. Le postazioni degli alunni possono essere utilizzate anche dai docenti il cui accesso è previsto senza credenziali.

Gestione accessi

Attualmente l’accesso ai dispositivi collegati alle LIM sono controllati dal docente e, sotto la sua diretta supervisione, possono essere utilizzati dagli alunni. Ogni docente accede al registro elettronico attraverso una password personale che non può essere comunicata a terzi. La stessa procedura viene utilizzata dalle famiglie, sempre attraverso l’accesso con password personali.

E-mail

Il docente fornisce l’indirizzo della propria posta elettronica alla scuola per ricevere e-mail informative da parte del Dirigente Scolastico e degli uffici di segreteria.

Sito web della scuola

La scuola attualmente ha un sito ufficiale con il seguente indirizzo web: “www.icriesi.edu.it”. Il SITO WEB rappresenta un’interfaccia con l’esterno ed è articolato in diversi settori. La gestione del sito è affidata al personale autorizzato dal D.S. (Animatore Digitale) per l’inserimento dei contenuti; quest’ultimi possono essere inseriti anche dai docenti sotto la supervisione dell’animatore digitale che ne cura la pubblicazione e del

DS.

Social network

Attualmente non si utilizzano social network nella didattica.

Protezione dei dati personali.

I docenti e il personale amministrativo compiono operazioni di trattamento dei dati personali nel rispetto delle norme previste in materia per fini burocratici e organizzativi. Eventuali usi eccezionali dei dati personali devono essere preventivamente autorizzati dai soggetti interessati o da chi esercita la patria potestà in caso di minori.

4. STRUMENTAZIONE PERSONALE

Per gli alunni

Il nostro Istituto Comprensivo è articolato in Scuola dell'Infanzia, Scuola Primaria e Scuola Secondaria di 1° grado, pertanto, l'utenza è costituita da alunni di età compresa tra 3 e 13 anni. È opportuno sviluppare le competenze digitali in termini di consapevolezza, responsabilità e normalità, in linea con le Indicazioni Nazionali per la scuola del primo ciclo, ma anche per un'opportunità che può venire dall'uso del mobile device personale nella prospettiva dell'attuazione della politica del BYOD. Gli alunni avranno la possibilità di utilizzare i dispositivi personali con il consenso dei genitori e solo su richiesta degli insegnanti. Per la scuola dell'Infanzia il divieto è categorico.

Per i docenti

I docenti possono utilizzare dispositivi personali e in dotazione della scuola esclusivamente per fini didattici. L'uso incauto dei dispositivi comuni può essere addebitato al responsabile del danno attraverso la tracciabilità dell'accesso. L'utilizzo dei dispositivi in uso e della rete WI-FI sarà autorizzato, previa richiesta e rilascio di credenziali di accesso, dal D.S. che ne valuterà la coerenza con gli scopi didattici garantiti dal richiedente. Il collegamento di qualsiasi dispositivo potrà essere monitorato e controllato attraverso software di gestione della rete.

Per il personale della scuola

È prevista l'elaborazione di un Regolamento che norma l'utilizzo della rete e dei dispositivi degli uffici di segreteria.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

Prevenzione

Rischi

I rischi effettivi che si possono correre a scuola nell'utilizzo delle TIC da parte degli alunni derivano da un uso non corretto delle tecnologie digitali personali e della scuola. Eludendo la sorveglianza degli insegnanti, gli alunni potrebbero anche scaricare e spedire foto personali o intime, proprie o di altri, video con contenuti indecenti o violenti, accedere a internet e a siti non adatti ai minori, ascoltare musica e giocare con i videogiochi non consigliati, leggere la posta elettronica e comunicare o chattare con sconosciuti, inviare o ricevere messaggi molesti e minacciosi. Il Cyberbullismo in particolare può originarsi anche dalla esasperazione di conflitti presenti nel contesto scolastico.

Azioni

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

- informare e formare i docenti, i genitori, il personale ATA e gli studenti sull'uso corretto delle nuove tecnologie;
- inserire nel PTOF specifiche attività di formazione sull'uso corretto e sicuro delle TIC;
- fornire ai genitori l'informativa e la richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori (es. liberatoria per la pubblicazione delle eventuali foto, immagini, testi e disegni relativi al proprio/a figlio/a);
- non consentire l'utilizzo arbitrario del cellulare personale degli alunni a scuola, in quanto per assolvere a ogni comunicazione urgente con i genitori o con chi ne fa le veci è sempre disponibile il telefono della scuola supervisionato dal personale addetto al centralino, che prima di passare la telefonata si accerta dell'identità dell'interlocutore;
- consentire l'utilizzo del cellulare sono in casi particolari ed eccezionali, individuati dagli insegnanti e autorizzati dal Dirigente Scolastico;

Rilevazione

Gli alunni possono mostrare segni di tristezza, di ansia, di risentimento nei confronti di compagni o di altri che “*allertano*” i docenti. Possono riferire, spontaneamente o su richiesta ai docenti fatti che possono essere accaduti anche al di fuori della scuola. Gli insegnanti possono venire a conoscenza di fatti o eventi personali e non inerenti al cyberbullismo confrontandosi periodicamente con gli alunni.

Che cosa segnalare

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

- contenuti afferenti alla privacy.

- contenuti afferenti all'aggressività o alla violenza.
- contenuti afferenti alla sessualità.

Si considerano da segnalare tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o un piccolo gruppo) tramite un utilizzo irresponsabile della tecnologia.

Come segnalare: quali strumenti e a chi

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 per conoscenza da restituire firmata (la segnalazione viene fatta a entrambe le famiglie se oltre alla vittima anche l'autore della condotta negativa è un altro alunno);
- convocazione scritta e colloquio con i genitori degli alunni, da parte dei Docenti e/o del DS;
- relazione scritta al Dirigente scolastico attraverso apposita scheda (*vedi allegato 1*);
- denuncia all'autorità giudiziaria ovvero agli organi di polizia territorialmente competenti.

La segnalazione deve essere supportata da quanto più specifiche prove e/o testimonianze.

È necessario conservare la prova che può essere presente nella memoria degli strumenti tecnologici utilizzati a scuola, può essere mostrata dall'alunno, può essere presentata da un reclamo dei genitori o notata dall'insegnante. In base all'urgenza le comunicazioni formali possono essere precedute da quelle informali, effettuate per le vie brevi.

Come gestire le segnalazioni a seconda dei casi

Casi	Gestione
Casi di "immaturità": può sembrare natural all'alunno fornire i propri dati sui siti allestiti in modo tale da attrarre l'attenzione dei bambini, con giochi e animazioni, personaggi simpatici e divertenti, che richiedono una procedura di registrazione.	Detti comportamenti sono controllati e contenuti dai docenti attraverso i normali interventi educativi, di richiamo al rispetto delle regole di convivenza civile e democratica, di rispetto degli altri, per evitare che possano degenerare, diventare pericolosi per sé o offensivi e minacciosi per gli altri.
Casi "quasi aggressivi": spesso si verificano tra coetanei, le interazioni animate o i contrasti verbali, o la presa in giro "per gioco", effettuata anche in rete, che mettono alla prova la relazione con i compagni, la supremazia o la parità tra i soggetti implicati e l'alternanza e sperimentazione dei diversi ruoli.	

Casi di Cyberbullismo: - invio di sms, messaggi in chat, e-mail offensive o di minaccia; - diffusione di messaggi offensivi ai danni della vittima, attraverso la divulgazione di sms o e- mail nelle mailing-list o nelle chat - line; - pubblicazione nel cyberspazio di foto o filmati che ritraggono prepotenze o in cui la vittima viene denigrata.	Gli interventi mirati sul gruppo classe sono gestiti in collaborazione dal consiglio di classe e d'intesa con le famiglie, con percorsi didattici specifici volti alla gestione positiva del conflitto (gruppi di discussione, rappresentazioni e attività di role-play sull'argomento, strategie del problem solving, ecc.) In situazioni particolarmente problematiche, la scuola convoca i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi. Promuove e supporta la richiesta delle famiglie rivolta ai Servizi Sociali dell'Ente Locale per la fruizione di servizi socio- educativi comunali e alla ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare).
Nei casi di abuso sessuale in cui l'alunno: - scarica o diffonde immagini o filmati di pornografia infantile; - è indotto a spogliarsi davanti alla webcam oppure a inviare tramite Internet o cellulare una fotografia che lo ritrae nudo; - subisce ricatti ed è costretto a non rivelare gli abusi.	La denuncia all'autorità giudiziaria o agli organi di Polizia, da parte degli insegnanti o del Dirigente scolastico, costituisce il passo necessario per avviare un intervento di tutela a favore della vittima e attivare un procedimento penale nei confronti del presunto colpevole. La scuola lavora insieme alle altre figure professionali e alle famiglie, scambiando informazioni e condividendo progetti e prassi operative, favorendo le occasioni di confronto e di dialogo.

6. Provvedimenti Disciplinari in supporto all'azione educativa della Scuola

	Che cosa segnalare (comportamento errato)	Sanzioni	Organo di intervento N.1	Organo di intervento N.2	Organo di intervento N.3	Azioni da intraprendere
1	Uso del cellulare in orario scolastico.	Richiamo verbale	<u>IL Docente</u> con segnalazione scritta e firmata da parte dello/a stesso/a del fatto accaduto in classe, in palestra, nei corridoi e durante i turni di vigilanza, <u>al Referente entro</u>	Il Referente al Dirigente Scolastico	Dirigente Scolastico	Il cellulare viene requisito per un mese presso l'ufficio di Presidenza, il genitore è tenuto ad andare a ritirarlo al termine della scadenza.

			<u>24 ore dall'accaduto</u>			
2	Uso del cellulare per riprendere senza autorizzazione scene di vita scolastica.	Richiamo verbale segnalazione dell'accaduto sul Registro Elettronico	<u>Il Docente</u> con segnalazione scritta e firmata da parte dello/a stesso/a del fatto accaduto in classe, in palestra, nei corridoi e durante i turni di vigilanza, <u>al Referente entro 24 ore dall'accaduto</u>	Il Referente al Dirigente Scolastico	Dirigente Scolastico	Il cellulare viene requisito per un mese. Si chiede l'intervento da parte della famiglia.
3	Uso di cellulare o PC per compiere atti di cyberbullismo o cyberstalking	Segnalazione dell'accaduto sul registro elettronico, Convocazione del Consiglio di classe straordinario.	<u>Il Docente</u> con segnalazione scritta e firmata da parte dello/a stesso/a del fatto accaduto in classe, in palestra, nei corridoi e durante i turni di vigilanza, <u>al Referente entro 24 ore dall'accaduto</u>	Il Referente al Dirigente Scolastico	Dirigente Scolastico	Convocazione della famiglia dell'alunno coinvolto ed eventuali interventi di operatori di Enti esterni.
4	Uso del PC per scaricare o visualizzare materiale non consentito.	Richiamo verbale, con particolari conseguenze, e segnalazione dell'accaduto sul Registro Elettronico	<u>Il Docente</u> con segnalazione scritta e firmata da parte dello/a stesso/a del fatto accaduto in classe, in palestra, nei corridoi e durante i turni di vigilanza, <u>al Referente entro 24 ore dall'accaduto</u>	Il Referente al Dirigente Scolastico	Dirigente Scolastico	Convocazione della famiglia dell'alunno coinvolto
5	Inosservanza delle Netiquette (regole di comportamento in rete)	Richiamo verbale con particolari conseguenze e segnalazione dell'accaduto sul Registro Elettronico	<u>Il Docente</u> con segnalazione scritta e firmata da parte dello/a stesso/a del fatto accaduto in classe, in palestra, nei corridoi e durante i turni di vigilanza, <u>al Referente entro</u>	Il Referente al Dirigente Scolastico	Dirigente Scolastico	Convocazione della famiglia dell'alunno coinvolto

			<u>24 ore dall'accaduto</u>			
6	Flaming (messaggi on line violenti e volgari mirati suscitare forti discussioni verbal in chat)	Segnalazione dell'accaduto sul registro elettronico. Convocazione del Consiglio di Classe Straordinario.	<u>Il Docente</u> con segnalazione scritta e firmata da parte dello/a stesso/a del fatto accaduto in classe, in palestra, nei corridoi e durante i turni di vigilanza, <u>al Referente entro 24 ore dall'accaduto</u>	Il Referente al Dirigente Scolastico	Dirigente Scolastico	Convocazione della famiglia dell'alunno coinvolto, intervento di organi competenti
7	Denigrazione /esclusione (pubblicazioni di pettegolezzi e commenti offensivi).	Segnalazione dell'accaduto sul registro elettronico, Convocazione del Consiglio di Classe straordinario.	<u>Il Docente</u> con segnalazione scritta e firmata da parte dello/a stesso/a del fatto accaduto in classe, in palestra, nei corridoi e durante i turni di vigilanza, <u>al Referente entro 24 ore dall'accaduto</u>	Il Referente al Dirigente Scolastico	Dirigente Scolastico	Convocazione della famiglia dell'alunno coinvolto, intervento di organi competenti.
8	Denigrazione e ingiurie in classe tra alunni	Richiamo verbale con particolari conseguenze e segnalazione dell'accaduto sul Registro Elettronico	<u>Il Docente</u> con segnalazione scritta e firmata da parte dello/a stesso/a del fatto accaduto in classe, in palestra, nei corridoi e durante i turni di vigilanza, <u>al Referente entro 24 ore dall'accaduto</u>	Il Referente al Dirigente Scolastico	Dirigente Scolastico	Convocazione della famiglia dell'alunno coinvolto, intervento di organi competenti.

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

Nelle pagine successive sono indicati gli allegati: Scheda 1- 2 – 3 – 4- 5 - 6. Essi rappresentano gli strumenti che utilizzeremo per gestire le infrazioni alla Policy, per assicurare la protezione dei dati personali, per rilevare, monitorare, gestire le segnalazioni e i casi rilevati.

Riesi, 15 ottobre 2019

Il Dirigente Scolastico

SCHEDA DI SEGNALAZIONE DEL FATTO ACCADUTO

(da trasmettere al Referente)

ORDINE DI SCUOLA:

- ☐ INFANZIA
- ☐ PRIMARIA
- ☐ SECONDARIA DI 1° GRADO

CLASSE: **SEZ:** plesso

DATA DELL'ACCADUTO: _____

LUOGO: _____

DOCENTE/I PRESENTE/I: _____

DESCRIZIONE DEL FATTO:

.....

.....

.....

.....

DATA.....

FIRMA DEL/I DOCENTE/I

Procedure operative per la gestione dei casi.

LINEE GUIDA PER ALUNNI

- ☐ Non comunicare mai a nessuno la tua password e periodicamente cambiala, usando numeri, lettere caratteri speciali.
- ☐ Mantieni segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della tua scuola.
- ☐ Non inviare a nessuno fotografie tue o di tuoi amici.
- ☐ Prima di inviare o pubblicare su un BLOG la fotografia di qualcuno, chiedi sempre il permesso.
- ☐ Chiedi sempre al tuo insegnante a scuola o ai tuoi genitori a casa il permesso di scaricare documenti da Internet.
- ☐ Chiedi sempre il permesso prima di iscriverti a qualche concorso o prima di riferire l'indirizzo della tua scuola.
- ☐ Quando sei connesso alla rete RISPETTA SEMPRE GLI ALTRI, ciò che per te è un gioco può rivelarsi offensivo per qualcun altro.
- ☐ Non rispondere alle offese ed agli insulti.
- ☐ Blocca i Bulli: molti Blog e siti social network ti permettono di segnalare i cyberbulli.
- ☐ Conserva le comunicazioni offensive, ti potrebbero essere utili per dimostrare quanto ti è accaduto.
- ☐ Se ricevi materiale offensivo (e-mail, sms, mms, video, foto, messaggi vocali) non diffonderlo, potresti essere accusato di cyberbullismo.
- ☐ Rifletti prima di inviare: ricordati che tutto ciò che invii su internet diviene pubblico e rimane per SEMPRE.
- ☐ Riferisci al tuo insegnante o ai tuoi genitori se qualcuno ti invia immagini che ti infastidiscono e non rispondere; riferisci anche al tuo insegnante o ai tuoi genitori se ti capita di trovare immagini di questo tipo su Internet.
- ☐ Se qualcuno su Internet ti chiede un incontro di persona, riferiscilo al tuo insegnante o ai tuoi genitori.
- ☐ Ricordati che le persone che incontri nella Rete sono degli estranei e non sempre sono quello che dicono di essere.
- ☐ Non è consigliabile inviare mail personali, perciò rivolgiti sempre al tuo insegnante prima di inviare messaggi di classe o ai tuoi genitori prima di inviare messaggi da casa.
- ☐ Non scaricare (download) o copiare materiale da Internet senza il permesso del tuo insegnante o dei tuoi genitori.

- ☐ Non caricare (upload) materiale video o fotografico nei siti web dedicati senza il permesso del tuo insegnante o dei tuoi genitori.

LINEE GUIDA PER INSEGNANTI

- ☐ Evitate di lasciare le e-mail o file personali sui computer o sul server della scuola, lo spazio è limitato e di uso comune.
- ☐ Salvate sempre i vostri lavori (file) in cartelle personali e/o di classe e non sul desktop o nella cartella del programma in uso. Sarà cura di chi mantiene il corretto funzionamento delle macchine cancellare file di lavoro sparsi per la macchina e al di fuori delle cartelle personali.
- ☐ Discutete con gli alunni della policy e-safety della scuola, di utilizzo consentito della rete, e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di Internet.
- ☐ Date chiare indicazioni su come si utilizza Internet, ed eventualmente anche la posta elettronica, e informateli che le navigazioni saranno monitorate.
- ☐ Ricordate di chiudere la connessione (e di spegnere il computer) alla fine della sessione di lavoro su Internet e disabilitare la navigazione su Internet del laboratorio (qualora sia stata attivata).
- ☐ Ricordate agli alunni che la violazione consapevole della policy e-safety della scuola, di utilizzo consentito della rete, comporta sanzioni di diverso tipo.
- ☐ Adottate provvedimenti “disciplinari”, proporzionati all'età e alla gravità del comportamento.
- ☐ Adottate interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi, di ridefinizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni;
- ☐ Nelle situazioni psico-socio-educative particolarmente problematiche, convocate i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi (sportello di ascolto psicologico gratuito attualmente attivo presso la scuola, Servizi Sociali per la fruizione di servizi socio-educativi comunali, ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare);
- ☐ Chiedete/suggerite di cancellare il materiale offensivo, bloccare o ignorare particolari mittenti, uscire da gruppi non idonei, cambiare indirizzo e-mail, ecc.
- ☐ Segnalate la presenza di materiale pedopornografico (senza scaricarlo o riprodurlo) alla Polizia Postale o al Telefono Azzurro.

- ☐ In caso di abuso sessuale rilevato anche attraverso i nuovi mezzi di comunicazione come internet o il cellulare, confrontatevi con i colleghi di classe e il Dirigente Scolastico, denunciate all'autorità giudiziaria o agli organi di Polizia.

CONSIGLI AI GENITORI PER UN USO RESPONSABILE DI INTERNET A CASA

Consigli generali

- ☐ Posizionate il computer in salone o in una stanza accessibile a tutta la famiglia.
- ☐ Evitate di lasciare le e-mail o file personali sui computer di uso comun.
- ☐ Concordate con vostro figlio le regole: quando si può usare internet e per quanto tempo...
- ☐ Inserite nel computer i filtri di protezione: prevenite lo spam, i pop-up pubblicitari, l'accesso a siti pornografici.
- ☐ Aumentate il filtro del “*parental controll*” attraverso la sezione sicurezza in internet dal pannello di controllo.
- ☐ Attivate il firewall (protezione contro malware) e antivirus.
- ☐ Mostratevi coinvolti: chiedete a vostro figlio di mostrarvi come funziona internet e come viene usato per scaricare e caricare compiti, lezioni, materiali didattici e per comunicare con l'insegnante.
- ☐ Incoraggiate le attività on-line di alta qualità: ricercare informazioni scientifiche, ricercare nuovi amici nel mondo.
- ☐ Partecipa alle esperienze on-line: naviga insieme a tuo figlio, incontra amici on-line, discuti gli eventuali problemi che si presentano.
- ☐ Comunicate elettronicamente con vostro figlio: inviate, frequentemente, E-mail, Instant Message.
- ☐ Spiegate a vostro figlio che la password per accedere ad alcune piattaforme è strettamente personale e non deve essere mai fornita ai compagni o ad altre persone.
- ☐ Stabilite ciò che ritenete inaccettabile (razzismo, violenza, linguaggio volgare, pornografia).
- ☐ Discutete sul tema dello scaricare file e della possibilità di ricevere file con virus.
- ☐ Raccomandate di non scaricare file da siti sconosciuti.
- ☐ Incoraggiate vostro figlio a dirvi se vedono immagini particolari o se ricevono e-mail indesiderate.
- ☐ Discutete nei dettagli le conseguenze che potranno esserci se vostro figlio visita deliberatamente siti non adatti, ma non rimproveratelo se compie azioni involontarie.
- ☐ Spiegate a vostro figlio che le password, i codici pin, i numeri di carta di credito e i numeri di telefono e i dettagli degli indirizzi e-mail sono privati e non devono essere dati ad alcuno.
- ☐ Spiegate a vostro figlio che non tutti in Internet sono chi realmente dichiarano di essere; di conseguenza i vostri ragazzi non dovrebbero mai accordarsi per appuntamenti senza consultarvi prima.

- ☐ Il modo migliore per proteggere vostro figlio è usare Internet con loro, discutere e riconoscere insieme i rischi potenziali.

Consigli in base all'età

Se tuo figlio ha meno di 8 anni

- ☐ Seleziona con molta attenzione i siti “sicuri”: ricordati che i gestori dei siti, per trarre il massimo guadagno, permettono agli inserzionisti di pubblicizzare i propri prodotti.
- ☐ Comunica a tuo figlio tre semplici regole:
 - ☐ non dare il tuo vero nome, indirizzo e numero di telefono. Usa sempre il tuo “computer username” o nickname;
 - ☐ se compare sullo schermo qualche messaggio o banner, chiudilo: insegna a tuo figlio come si fa;
 - ☐ naviga esclusivamente sui siti autorizzati dai genitori: se vuoi andare su un nuovo sito, dobbiamo andarci INSIEME (molti siti richiedono la registrazione. Insegna a tuo figlio come registrarsi senza rivelare informazioni personali).

Se tuo figlio ha tra gli 8 anni e i 13 anni

- ☐ Progressivamente diminuisci la supervisione: dagli otto ai dieci anni permetti a tuo figlio di navigare da solo nei siti autorizzati, sottolineando che deve consultarti prima di esplorarne dei nuovi.
- ☐ Verifica periodicamente i contenuti dei siti “sicuri”.
- ☐ Discuti con tuo figlio i rischi che possono presentarsi durante la navigazione on-line.
- ☐ Controlla, dalla cronologia il menu navigazione, se tuo figlio ha consultato siti non autorizzati per i quali non ti ha chiesto il permesso.

Supervisiona l'e-mail di tuo figlio dopo averlo reso consapevole del fatto che hai pieno accesso alle sue comunicazioni. Se tuo figlio vuole usare IM verifica che i suoi contatti siano limitati agli amici conosciuti. Specifica che non può inserire nuovi contatti senza averti prima consultato.

- ☐ Comunicagli che è assolutamente vietato cliccare su un link, contenuto in una E-mail, su un pop-up pubblicitario o su un banner (ricordati, infatti, che potrebbero presentarsi immagini pornografiche che potrebbe avviarsi il download di “malware”).
- ☐ Incoraggia l'uso di internet per svolgere ricerche scolastiche. Definisci il tempo massimo di connessione ed incoraggia le attività con il mondo reale.

Il/La sottoscritto/a _____ nato/a a _____ prov. _____ il _____

Residente a _____ via _____ n. _____ CAP _____

codice fiscale _____ e-mail _____

in qualità di:

☐ docente scuola dell'infanzia ☐ docente scuola primaria ☐ personale ATA altro

☐ personale autorizzato: _____

chiede

l'autorizzazione per accedere ad Internet tramite la rete wireless o cablata dell'Istituto.

In particolare si impegna a:

- Non scaricare/duplicare/distribuire software o altri contenuti protetti da diritto d'autore.
- Non accedere a siti o risorse dal contenuto illegale o non consono alle regole di comportamento dettate dal carattere istituzionale ed educativo della scuola.
- Non diffondere virus o altri software malevoli all'interno della rete e a dare immediato avviso all'Amministrazione di comportamenti anomali o di virus riconosciuti.
- Avere cura che le credenziali di accesso alla rete non vengano comunicate a terzi.
- Si ricorda, inoltre, che l'accesso attraverso l'autenticazione trasferisce direttamente la responsabilità degli atti commessi durante la navigazione a colui che esercita tale operazione.

Altre notifiche:

- In caso di accesso con un proprio dispositivo, l'Istituto non potrà essere ritenuto in alcun modo responsabile per eventuali danni legati alla fruizione del servizio di rete.
- L'accesso alla rete wireless non è garantito e può subire limitazioni, sospensioni, blocchi, dipendenti o meno dalla volontà dell'Istituto. In nessun caso l'utente potrà rivalersi sull'Istituto per il mancato servizio.
- Il servizio wireless viene fornito con limitazioni definite sul numero di accessi contemporanei, con la conseguenza che non si verifichino situazioni di sovraccarico della rete.
- L'autorizzazione all'uso della rete di Istituto potrà venire revocata (cancellazione dell'utente) in qualsiasi momento per cause tecniche o per motivazioni legate all'uso improprio o alla violazione delle norme di comportamento.

CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

Manifesto il consenso, in qualità di genitore/tutore, espresso ai sensi dell'ex art. 13 D. Lgs. 196/03, al trattamento ed alla comunicazione dei dati personali di mio figlio/a da parte della scuola, nei limiti, per le finalità e con le modalità stabilite dalla legge.

☐ ACCONSENTO

☐ NON ACCONSENTO

Firma del Genitore o di chi ne fa le veci _____

1. CONSENSO DA PARTE DEI GENITORI PER L'ACCESSO AD INTERNET

Reso dai genitori degli alunni minorenni (D. Lgs. 196/2003 “Codice in materia di protezione dei dati personali”)

Il sottoscritto/a _____ nato/a a _____ il _____
 residente a _____ via _____ n. _____
 genitore dell'alunno/a _____ frequentante la classe _____ sez. _____
 plesso _____

☐ ACCONSENTO

☐ NON ACCONSENTO

Firma del Genitore o di chi ne fa le veci _____

LIBERATORIA PER LA PUBBLICAZIONE DI FOTOGRAFIE E RIPRESE VIDEO ANCHE SU INTERNET

Il sottoscritto genitore/tutore acconsente che siano realizzate immagini (foto, filmati, CD, DVD) che includono il/la proprio/a figlio/a, per fini didattici (mostre, partecipazioni a concorsi ed eventi, ecc.), consapevole che le medesime potranno essere distribuite anche ad altri alunni interessati. Si impegna, inoltre, ad utilizzare, a sua volta, il suddetto materiale, per esclusivo uso domestico e a non diffonderlo su Internet senza autorizzazione. Inoltre, il genitore solleva la scuola da ogni responsabilità derivante dall'uso improprio di terze parti.

☐ ACCONSENTO

☐ NON ACCONSENTO

Firma del Genitore o di chi ne fa le veci _____