Centro esami 32011

Ministero dell'Istruzione, dell'Università e della Ricerca
Ufficio Scolastico Regionale per il Lazio
Istituto comprensivo "via Acquaroni"
Via Acquaroni, 53 00133 ROMA tel. 062050607 fax 0620449294
Mail: rmic8e700q@istruzione.it Pec: rmic8e700q@pec.istruzione.it
Codice Fiscale. 97713360580 – DIS. XVI
Sito web http://www.istitutocomprensivoacquaroni.gov.it/

E-safety policy

Redatto:

Anno scolastico 2017/2018

Indice E-Safety Policy

E-SAFETY POLICY " I.C. Via Acquaroni"

1.Introduzione

Scopo della Policy

Il presente documento ha lo scopo di descrivere le norme comportamentali e le procedure per l'utilizzo delle ICT nell'Istituto Comprensivo "Via Acquaroni" di Roma, 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, nello specifico, si impegna a :

1. adottare le misure atte a facilitare e a promuovere l'uso delle ICT nella didattica e negli ambienti scolastici;

2. stabilire le misure di prevenzione e di gestione di situazioni problematiche relative all'uso delle tecnologie digitali.

Grazie a un percorso guidato e al materiale di supporto messo a disposizione sul sito del progetto www.generazioniconnesse.it, si definiscono qui le misure che l'Istituto intende adottare:

- per la promozione dell'utilizzo delle ICT nella didattica;
- per la prevenzione, ovvero le azioni finalizzate alla prevenzione di fenomeni legati ai rischi delle tecnologie digitali;
- per la segnalazione dei casi, ovvero le disposizioni semplici su come segnalare i casi nella scuola;
- per la gestione dei casi, ovvero le misure che la scuola intende attivare a supporto delle famiglie e degli studenti che sono stati vittime o spettatori attivi e/o passivi di quanto avvenuto.

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

Nell'ambito di questa policy sono individuati i seguenti ruoli e le principali responsabilità correlate:

1. Dirigente scolastico:

- garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- garantire ai propri docenti una formazione di base sulle Tecnologie dell'Informazione e della Comunicazione (ICT) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse;

· garantire l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on line;

2. Animatore digitale, come da PNSD:

· *Formazione interna* - stimolare la formazione interna alla scuola negli ambiti del PNSD, attraverso l'organizzazione di laboratori formativi, favorendo l'animazione e la partecipazione di tutta la comunità scolastica alle attività formative, come ad esempio quelle organizzate attraverso gli snodi formativi;

· *Coinvolgimento della comunità scolastica* - favorire la partecipazione e stimolare il protagonismo degli studenti nell'organizzazione di workshop e altre attività, anche strutturate, sui temi del PNSD, anche attraverso momenti formativi aperti 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 (es. uso di particolari strumenti per la didattica di cui la scuola si è dotata; adozione di metodologie comuni; informazione su innovazioni esistenti in altre scuole; laboratorio di robotica educativa e pensiero computazionale), coerenti con l'analisi dei fabbisogni della scuola stessa, anche in sinergia con attività di assistenza tecnica condotta da altre figure (team dell'innovazione, gruppo SNODO, personale tecnico esterno).

3. 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, controllando al contempo che le norme di sicurezza vengano rispettate;

· facilitare la trasmissione di comunicazioni relative alle tecnologie digitali tra le varie componenti della scuola (Dirigente scolastico, Animatore digitale, team dell'innovazione, gruppo SNODO, tecnici esperti esterni ,assistenti esterni per il registro elettronico, docenti e famiglie degli alunni);

· curare la registrazione dei disservizi e delle problematiche relative alla rete e all'uso del digitale segnalate dai docenti, provvedendo all'intervento del personale tecnico di assistenza.

4. Docenti:

· provvedere alla propria formazione/aggiornamento sull'utilizzo del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in Internet e dell'immagine degli altri: lotta al cyberbullismo);

· sviluppare le competenze digitali degli alunni e fare così in modo che conoscano e seguano le norme di sicurezza nell'uso del web e utilizzino correttamente le tecnologie digitali sia a scuola sia nelle attività didattiche extracurricolari;

· segnalare prontamente alle famiglie eventuali problematiche emerse in classe nell'utilizzo del digitale e stabilire comuni linee di intervento educativo per affrontarle;

· segnalare al Dirigente scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di infrazione.

5. Alunni/studenti:

· 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 nello svolgimento dei compiti a casa per mezzo del digitale, qualora insorgano difficoltà o dubbi nel suo utilizzo.

6. Genitori:

· contribuire, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;

· incoraggiare l'impiego delle ICT da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza;

· agire in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite.

Condivisione e comunicazione della Policy all'intera comunità scolastica

a) Condivisione e comunicazione della Policy agli alunni:

· All'inizio dell'anno scolastico i docenti si occuperanno di illustrare agli alunni, oltre al regolamento d'Istituto, anche questa policy, sottolineando l'importanza educativa insita in essa.

· Nel corso dell'anno saranno dedicate da ciascun docente alcune lezioni alle buone pratiche per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta al cyberbullismo.

b) Condivisione e comunicazione della Policy al personale:

· Le norme adottate dalla scuola in materia di sicurezza nell'utilizzo del digitale saranno discusse in tutti gli organi collegiali e rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito web della scuola.

· Il personale della scuola riceverà un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso materiali resi disponibili anche sul sito web della scuola.

c) Condivisione e comunicazione della Policy ai genitori:

· Le famiglie saranno informate in merito alla linea di condotta adottata dalla scuola per un uso sicuro e responsabile delle tecnologie digitali e di internet attraverso la condivisione del presente documento e di materiali informativi specifici sul sito web della scuola.

· 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.

Gestione delle infrazioni alla Policy.

In relazione a quanto specificato in questa policy le infrazioni saranno gestite in modo graduale rispetto alla gravità dell'infrazione e, nel caso degli alunni, anche alla loro età.

Infrazioni degli alunni.

È bene che i docenti introducano, preventivamente, attività laboratoriali miranti a sviluppare nei loro alunni una sempre maggiore consapevolezza dei rischi legati a un uso imprudente e improprio del web e che forniscano loro, ogniqualvolta avvenga un'infrazione alle regole stabilite, gli strumenti per affrontare le conseguenze dei loro errori.

I provvedimenti disciplinari da adottare da parte del consiglio di classe nei confronti dell'alunno che ha commesso un'infrazione alla policy (in proporzione sia all'età dello studente sia alla gravità dell'infrazione commessa) saranno i seguenti:

· richiamo verbale;

· sanzioni estemporanee commisurate alla gravità della violazione commessa (assegnazione di attività aggiuntive da svolgere a casa su temi di Cittadinanza e Costituzione; divieto temporaneo di prendere parte alla ricreazione e simili);

- 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; rimozione temporanea dei diritti di accesso a internet
- presa in custodia del dispositivo
- sospensione con obbligo di frequenza con il coinvolgimento in attività socialmente utili all'Istituzione Scolastica
- allontanamento temporaneo dalle lezioni
- segnalazione alle autorità competenti.

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.

Infrazioni dei genitori.

Compito precipuo dei genitori è supportare gli insegnanti e il personale scolastico nel riconoscimento e nella costruzione di azioni di contrasto efficaci ai principali rischi rappresentati dalla navigazione in internet di utenti molto giovani e spesso poco accorti. Nel caso di infrazione si prevedono interventi, rapportati alla sua gravità, che vanno dalla semplice comunicazione del problema alla convocazione da parte dell'insegnante di classe o del Dirigente Scolastico.

Monitoraggio dell'implementazione della Policy e suo aggiornamento.

Il monitoraggio dell'implementazione/aggiornamento della Policy avverrà

- alla fine di ogni anno scolastico, contestualmente alle indicazioni di casi rilevati e non preventivamente considerati nell'e-safety;
- all'inizio di ogni anno scolastico, contestualmente alla revisione del PTOF, a cura del Dirigente scolastico, dell'Animatore digitale e dei collaboratori del Dirigente, anche attraverso la somministrazione ad alunni/e personale scolastico di questionari atti a verificare l'insorgenza di nuove necessità e la revisione di tecnologie esistenti.

Integrazione della Policy con Regolamenti esistenti.

Il presente documento si integra pienamente con obiettivi e contenuti dei seguenti documenti, che specificano il contesto di attuazione delle politiche dell'Istituto Comprensivo per un uso efficace e consapevole del digitale nella didattica:

- PTOF, incluso il piano per l'attuazione del PNSD;
- POF;
- Regolamento interno d'Istituto;
- Regolamenti dei laboratori presenti nell'Istituto.

2. Formazione e curriculo

Curriculo sulle competenze digitali degli alunni/studenti

La competenza digitale, inserita tre le otto competenze chiave a livello europeo, prevede, oltre al raggiungimento delle abilità di base delle TIC, anche implicazioni cognitive e relazionali.

La dimensione cognitiva comprende abilità legate al trattamento dell'informazione, dalla capacità di accedere, selezionare e interpretare dati a quella di valutarne criticamente la pertinenza e l'affidabilità. **La dimensione etica,** spesso trascurata,

riguarda il saper interagire con gli altri in modo corretto e responsabile, la circolazione del sapere online e il rispetto dei diritti di proprietà intellettuale, il tema dell'accessibilità e dell'inclusione. Comprende alcune delle tematiche più attuali rispetto al tema delle nuove tecnologie, dalla tutela della privacy al contrasto del fenomeno del cyberbullismo, e quelle che riguardano la dimensione relazionale ed affettiva dell'utilizzo di internet (la mancanza di un reale contatto visivo e/o fisico abbassa timidezze e inibizioni con quel che ne consegue...). Dalla integrazione di queste tre principali dimensioni emerge un concetto di competenza digitale denso, che fa riferimento alla capacità di comprendere e sfruttare l'effettivo potenziale delle tecnologie come costruzione di conoscenza e di promozione della partecipazione e dell'inclusione. La competenza nell'uso consapevole, critico e creativo delle nuove tecnologie diventa quindi una componente fondamentale nell'ottica della Cittadinanza digitale, trasversale al curriculum scolastico di ogni alunno/studente.

Per i suddetti motivi il nostro Istituto, nell'ambito del PNSD, già da tempo, ha proposto attività laboratoriali interne ed esterne, come la Settimana del Codice, Robotics School, il pensiero computazionale, uso dei libri di testo in formato digitale, utilizzo di classi virtuali. Il nostro Istituto ha incrementato la rete wi-fi e ampliato la dotazione di LIM e tablet; ha intrapreso un inizio di politica di BYOD; ha progettato e realizzato un'aula 3.0 e una 2.0 con attività legate ad esse, come laboratori di scrittura creativa e la formazione di un blog.

L'Istituto ha organizzato incontri con la Polizia di Stato (nell'ambito del progetto "Scuole Sicure") e i Carabinieri di zona per far comprendere i concetti di prevenzione e sicurezza, di bullismo e cyberbullismo e per illustrare le modalità con cui chiedere aiuto se si presentano situazioni di pericolo. E' stata richiesta anche la presenza della Guardia di Finanza, nell'ambito del progetto di "Educazione alla legalità economica".

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

Nell'ambito del PNSD il nostro Istituto ha previsto le figure dell'animatore digitale e del team dell'animazione, formati come previsto. Così come i docenti partecipanti all'aggiornamento dello Snodo formativo.

Il resto del corpo docente, sempre disponibile ad aggiornarsi, ha partecipato e parteciperà a corsi e/o attività di formazione organizzate dall'istituzione o dalle scuole associate in rete di ambito. Il percorso prevede e prevederà:

- incontri di formazione all'utilizzo dello scrutinio elettronico
- corsi on-line
- momenti di autoaggiornamento
- momenti di formazione personale e/o collettiva organizzati dall'AD, team e snodo
- partecipazione a iniziative promosse dalle scuole in rete di ambito o dal MIUR

- visione e fruizione di materiali messi a disposizione sul sito della scuola, riguardanti l'utilizzo e l'integrazione delle TIC nella didattica
- monitoraggio del gradimento e dei risultati conseguiti

Tutte le azioni realizzate finora e da mettere in atto in futuro si auspica che esortino i docenti a utilizzare e integrare sempre di più e costantemente le TIC nella didattica.

Formazione dei docenti sull'utilizzo consapevole e sicuro di internet e delle tecnologie digitali

L'avvio del progetto "Generazioni connesse" ha rappresentato una reale opportunità di rendere coesa e unitaria la formazione on-line dei docenti sull'uso consapevole e sicuro della rete e delle tecnologie digitali. Si è predisposto nel sito web dell'Istituto uno spazio denominato "Legalità, bullismo e cyberbullismo" in cui i docenti potranno trovare materiale informativo sull'argomento, guide in pdf, manuali e link utili all'autoaggiornamento, oltre ai corsi tematici online messi a disposizione dalla piattaforma "Generazioni connesse". Si prevede di fornire indicazioni a tutto il personale scolastico sulla e-safety policy dell'Istituto. Per l'anno prossimo sono previsti momenti di formazione e autoaggiornamento organizzati dal Referente per il contrasto e la prevenzione al bullismo e al cyberbullismo, in collaborazione con Animatore Digitale, team e snodo (anche con intervento di esperti esterni.)

Sensibilizzazione delle famiglie

Il nostro Istituto Comprensivo nell'anno scolastico 2017/2018 ha aperto uno sportello di ascolto gestito da uno psicologo, nell'ambito del progetto "Camminiamo insieme…". Lo sportello risponde a richieste di consulenza di studenti della scuola superiore di 1 grado, di genitori e docenti, inerenti a tematiche di difficoltà/disagio reazionale e sospetti episodi di bullismo. Ha attuato, inoltre, nella scuola primaria dei laboratori esperienziali rivolti agli alunni delle quarte e delle quinte classi. Data l'affluenza elevata, si prospetta per il prossimo anno scolastico un'incentivazione dell'attività e della presenza a scuola.

Il corpo docente, dopo la formulazione dell'E-Safety Policy d'Istituto, si propone di attuare le seguenti azioni :

- Comunicazione e presentazione ai genitori del Regolamento della Policy, con l'intervento della Polizia di Stato
- Fornire periodicamente leaflet informativi sull'argomento
- Fornire informazioni sui siti nazionali di sostegno per i genitori,quali il sito www.generazioniconnesse.it

- Informare e formare sull'uso consapevole della rete e sui pericoli derivanti da una scarsa conoscenza della stessa in occasione di incontri scuola-genitori per condividere con essi regole comuni.

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

Accesso ad Internet: filtri antivirus e sulla navigazione

La scuola è presente sulla rete con un portale web costantemente aggiornato contenente informazioni utili per il personale scolastico e per le famiglie.

L'I.C. da quest'anno è dotato di una connessione web tramite fibra ottica che serve tutti i plessi di scuola primaria e secondaria di primo grado. La scuola dell'infanzia non è copertada connessione internet.

L'accesso ad internet è consentito esclusivamente per scopi didattici.

I plessi della scuola primaria e secondaria sono dotati di laboratori di informatica i cui computer sono interconnessi tramite un sistema di rete lan.

Mentre i laboratori della scuola primaria sono sufficientemente attrezzati, quelli della scuola secondaria, soprattutto quelli del plesso di via Merlini, risultano sprovvisti ed obsoleti. Il plesso è però attrezzato con un laboratorio 3.0 che presenta Lim, tablet e televisore touch in cui è possibile strutturare lezioni interamente a carattere digitale.

Ogni classe della scuola primaria è dotata di un tablet ed è presente una Lim per ogni gruppo di classi parallele.

Di tutti i dispositivi presenti nell'I.C., solo i portatili che sono nuovi sono protetti da antivirus e non sono attive funzioni di parental control.

I servizi di manutenzione e di assistenza informatica sono gestiti dalla società Infotek s.a.s., che assolve alle segnalazioni entro tre giorni lavorativi.

Le criticità da affrontare nei prossimi tre anni sono diverse. Nello stabilire quali saranno gli obiettivi da raggiungere, sicuramente bisognerà tenere presente la necessità di implementare i laboratori della scuola secondaria, di installare software antivirus e impostare le necessarie funzioni di sicurezza e filtri per garantire ai nostri studenti la possibilità di navigare in totale sicurezza.

Gestione accessi (password, backup, ecc.)

L'accesso al sistema informatico per la didattica, server e internet,nel laboratorio multimediale è consentito al personale docente attraverso l'utilizzo del nome utente della scuola e password univoci. I docenti registrano il proprio accesso scrivendo sugli appositi registri la data, l'orario di utilizzo dei laboratori ed eventuali annotazioni su riscontri di malfunzionamenti della strumentazione. Non vi è un backup dei file elaborati, se non quello operato dai docenti interessati su supporti rimovibili personali. Le postazioni del laboratorio funzionano come stazioni di lavoro e non come archivi.

E–mail

L'account di posta elettronica è solo quello istituzionale ed è utilizzato unicamente per comunicazioni, in entrata e in uscita, di carattere lavorativo. Gli utenti si impegnano a non diffondere informazioni che possono nuocere alla reputazione della scuola o essere contrarie alla morale o alle leggi in vigore.

Blog e sito web della scuola

Il Sito web della scuola è il punto di riferimento per tutti gli aggiornamenti sui progetti, la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy. La scuola attualmente è dotata di un sito istituzionale con estensione "gov.it". Esso è stato lanciato nell'a.s. 2015/16 dal web master esterno Nicolas Pascali (Infotek S.a.s.), utilizzando i contenuti e le pagine create e lanciate precedentemente dall'attuale animatore digitale. Il web master ha cura di effettuare aggiornamenti e backup periodici e interviene in caso di emergenza.

1. Sul sito web sono presenti: l'indirizzo della scuola, e-mail e numero di telefono.
2. Le varie pagine, compresa la home del sito, vengono aggiornate quasi quotidianamente dall'Animatore Digitale, che ne valuta, con il Dirigente Scolastico, la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, nel rispetto della privacy.
3. L'area relativa alle circolari è gestita ed aggiornata dal personale di Segreteria, individuato ed incaricato per specifiche competenze tecnico-informatiche.

Il sito prevede un'area pubblica, per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, le iniziative, le scadenze ministeriali, avvisi di carattere generale, e delle aree riservate, accessibili solo dopo autenticazione con password diversificate:

o *per i docenti e il personale ATA*: che possono visualizzare le circolari e la modulistica.
o *per i membri del consiglio d'Istituto*: che possono visualizzare verbali o piani annuali non ancora deliberati.
o *per il MIUR*: che può visionare materiale strettamente riservato non pubblico.

Tra i contenuti pubblici, accessibili ai visitatori e suddivisi per argomenti, è possibile trovare regolamenti, materiali didattici, pubblicizzazione di eventi, documentazione di attività curricolari ed extracurricolari svolte e la bacheca sindacale(RSU). Nell'area "presentazione dell'Istituto" ogni anno viene realizzato e caricato su You-tube il video rappresentativo dei progetti svolti nei tre ordini di scuola. Le fotografie e i video pubblicati includono allieve e allievi le cui famiglie hanno concesso opportuna autorizzazione. All'atto dell'iscrizione infatti è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico di immagini e video delle/dei minori secondo i principi sopra indicati. L'Animatore digitale ha inoltre predisposto banner (pulsanti) attivi che permettono l'accesso a link di interesse tra cui quello di "Classeviva"(registro elettronico, le credenziali di accesso vengono fornite alle

famiglie all'inizio del 1°anno scolastico nell'Istituto), "Programma il Futuro" (per diffondere concetti di base dell'informatica attraverso la programmazione coding), "Generazioni Connesse" (per la prevenzione e il contrasto al bullismo e al cyberbullismo a scuola), "Scuola in chiaro" (per cercare le scuole, esaminare e confrontare le caratteristiche). Il sito web dell'Istituto offre, inoltre, altri servizi alle famiglie ed agli utenti esterni, quali consultazione del PTOF; Sportello di ascolto; Biblioteca scolastica multimediale; Regolamento d'Istituto; Albo on line; Amministrazione trasparente; Servizio mensa (con i menu diversificati per la sezione primavera/ponte, scuola dell'infanzia, scuola primaria e secondaria di primo grado); ed altre informazioni generali sulla scuola.

- Tra i progetti futuri è contemplata la possibilità di aprire un Blog con il software wordpress.com a scopo didattico collaboratoriale con la partecipazione attiva degli studenti che sarà utilizzato per scambio di informazioni e materiale.

Social Network e protezione dei dati personali

Attualmente la scuola non è presente sui più diffusi social network quali Facebook, Twitter e Instagram né per scopi didattici né per promuovere le iniziative della scuola e il personale scolastico non è autorizzato ad utilizzarli a nome e/o per conto dell'istituzione scolastica.

È in uso il canale Youtube "Scuola Acquaroni", gestito unicamente dall'animatore digitale, la quale provvede a caricare video della durata non superiore a quattordici minuti, durata massima consentita per poter usufruire della pubblicazione gratuita.

Attualmente, alcuni docenti stanno sperimentando l'utilizzo di piattaforme didattiche quali HUB scuola e Edmodo.

Protezione dei dati personali

Per la protezione dei dati personali, il principale riferimento normativo è il Decreto Legislativo 30 giugno 2003, n.196 (Codice della Privacy).Tuttavia, si possono individuare al riguardo alcune linee guida di e-safety.

All'interno dell'istituzione scolastica, il responsabile della gestione del trattamento dei dati personali è il Dirigente Scolastico, il quale indica nella persona del DSGA e nel personale amministrativo gli incaricati al trattamento di tali dati.

Il suddetto personale è istruito sulla procedura da seguire per segnalare eventuali incidenti in cui la protezione dei dati potrebbe essere stata compromessa, ad usare sistemi di logout al momento di lasciare i computer utilizzati e ad impostare il lockout (bloccaggio) dopo un certo periodo di inattività.

La segreteria utilizza password nelle postazioni informatiche di lavoro, individua soggetti preposti alla gestione delle password, ha un codice identificativo personale per ogni utente, utilizza programmi antivirus, protegge e regolamenta gli accessi locali che ospitano i dati riservati o in cui si trovano le postazioni di lavoro che ne consentono l'accesso, definisce i criteri per garantire l'integrità e la trasmissione

sicura dei dati e si dota di mezzi elettronici adeguati per impedire l'accesso dall'esterno alla propria rete.

Lo smaltimento di qualsiasi apparecchiatura deve essere conforme alle norme di smaltimento dei rifiuti elettrici ed elettronici e per qualsiasi server contenente dati personali o soggetti alla tutela della privacy è necessario un certificato di cancellazione sicura.

Il personale della scuola può condividere numeri di telefono personali o indirizzi di posta elettronica privati con la componente studentesca e con i genitori, solo in casi limitati relativi a scopi didattici e organizzativi. Per la regolare e quotidiana comunicazione scuola-famiglia è attivo un numero telefonico per ogni plesso dell'Istituto e un indirizzo e-mail, entrambi presenti sul sito istituzionale.

Le fotografie o i video da pubblicare sul sito che includano alunni e alunne saranno selezionati con cura e non permetteranno l'identificazione dei singoli attraverso l'indicazione del nome, a meno che non si tratti di eventi particolari per cui le famiglie potranno concedere opportuna autorizzazione. Si preferirà l'utilizzo di fotografie o video di gruppo. All'atto dell'iscrizione, è richiesto alle famiglie di firmare un'autorizzazione per consentire l'uso didattico di immagini e video dei minori secondo i principi sopra indicati. Ogni caso particolare sarà preso in considerazione per stabilire l'opportunità di pubblicare dati personali e sarà presentata apposita richiesta circostanziata che avrà valore solo per lo specifico evento.

Nell'anno 2016, il Garante per la Privacy ha pubblicato l'opuscolo "La scuola a prova di privacy", in cui sono indicate le linee guida da seguire riguardo il trattamento dei dati personali all'interno della comunità scolastica. Tutte le scuole hanno l'obbligo di far conoscere agli studenti, alle famiglie e ai docenti le modalità di trattamento dei loro dati personali.

Le istituzioni scolastiche pubbliche possono trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali oppure quelli espressamente previsti dalla normativa di settore. Per tali trattamenti, non sono tenute a chiedere il consenso degli studenti. Alcune categorie di dati personali degli studenti e delle famiglie, come quelli sensibili e giudiziari, devono essere trattate nel rispetto di specifiche norme di legge, verificando prima non solo la pertinenza e completezza dei dati, ma anche la loro indispensabilità rispetto alle finalità di rilevante interesse pubblico che si intendono perseguire.

Ogni persona ha diritto di conoscere se sono conservate informazioni che la riguardano, di apprenderne il contenuto, di farle rettificare se erronee, incomplete o non aggiornate. Per esercitare questi diritti è possibile rivolgersi direttamente al "titolare del trattamento", anche tramite i suoi incaricati o responsabili del trattamento dei dati. Se non si ottiene risposta o se il riscontro non risulta adeguato, è possibile rivolgersi al Garante o alla magistratura ordinaria.

L'accesso agli atti amministrativi è regolato dalla singola amministrazione che deve valutare l'esistenza di presupposti normativi che permettono di prendere visione e di estrarre copia dei documenti amministrativi ai soggetti con un "interesse diretto, concreto e attuale" alla conoscibilità degli atti.

Le istituzioni scolastiche devono prestare particolare attenzione a non diffondere, anche per mero errore materiale, dati idonei a rivelare lo stato di salute degli studenti, così da non incorrere in sanzioni amministrative o penali.

L'utilizzo di telefoni cellulari e di apparecchi per la registrazione di suoni e immagini è disciplinato dal Regolamento di Istituto pubblicato sul sito della scuola. Tuttavia nessun membro della comunità scolastica, in alcuna occasione (ad esempio, all'interno della scuola o durante un'uscita didattica), può diffondere o comunicare sistematicamente i dati di altre persone (ad esempio pubblicandoli su Internet) senza averle prima informate adeguatamente e averne ottenuto l'esplicito consenso.

Le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici non violano la privacy. Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale e non alla diffusione. Va, però, prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini su Internet. In caso di comunicazione sistematica o diffusione diventa infatti necessario, di regola, ottenere il consenso informato delle persone presenti nelle fotografie e nei video dei genitori (o di chi ne fa le veci) nel caso di minori.

Le scuole di ogni ordine e grado sono soggette a un regime di pubblicità e trasparenza. È però necessario che gli istituti scolastici prestino particolare attenzione a non rendere accessibili informazioni che dovrebbero restare riservate o a mantenerle on line oltre il tempo consentito, mettendo in questo modo a rischio la privacy e la dignità delle persone a causa di un'errata interpretazione della normativa o per semplice distrazione.

4. Strumentazione personale

Per gli studenti: gestione degli strumenti personali – cellulari, tablet, ecc.

E'consentito agli alunni della Scuola dell'Infanzia, Primaria e Secondaria di primo grado di portare a scuola macchine fotografiche o Mp3 privi di connessione dati, da utilizzare durante le uscite didattiche, e dispositivi che rientrino tra gli strumenti compensativi per lo svolgimento delle attività didattiche previste (BYOD) e/ o per attività programmate che coinvolgono tutti gli alunni.

La scuola sconsiglia agli alunni della Scuola Secondaria di I° grado di portare il telefono mobile a scuola. Ciò è comunque consentito per motivi familiari e organizzativi. Coerente con quanto indicato dalla Direttiva Ministeriale n° 30 del 15 marzo 2007, gli studenti sono però tenuti a tenere il telefono spento durante tutto il periodo di permanenza a scuola e in ogni ambiente. A tale disposizione fa eccezione il caso in cui l'uso sia espressamente autorizzato da un docente di classe per lo svolgimento di attività educative/didattiche riguardanti la scuola o in casi di estrema e comprovata urgenza per comunicazioni tra gli alunni e le famiglie. Ogni studente è responsabile del proprio dispositivo e non può prendere in prestito dispositivi di altri. L'uso improprio verrà sanzionato in base alla normativa vigente in materia.

Per i docenti: gestione degli strumenti personali – cellulari, tablet, ecc.

Durante le ore di lezione, ai docenti non è consentito l'utilizzo del cellulare che non deve essere lasciato incustodito e non può essere prestato agli alunni. A tale disposizione fa eccezione il caso in cui l'uso di dispositivi elettronici personali sia unicamente a scopo didattico e a integrazione dei dispositivi scolastici disponibili. Durante il restante orario di servizio l'uso del cellulare è consentito solo per comunicazioni personali che rivestano carattere di urgenza.L'uso improprio verrà sanzionato in base alla normativa vigente in materia.

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

Durante l'orario di servizio al restante personale scolastico l'uso del cellulare è consentito per comunicazioni personali urgenti. L'uso di altri dispositivi elettronici personali è permesso solo per attività funzionali al servizio e preventivamente autorizzato. L'uso improprio verrà sanzionato in base alla normativa vigente in materia.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

Prevenzione: Rischi e Azioni.

Il telefono cellulare o lo smartphone non sono richiesti dalla scuola, perché non sono ritenuti indispensabili in ambito scolastico, ma vengono forniti dai genitori degli alunni soprattutto per mantenere la comunicazione diretta con i figli anche fuori dal contesto scolastico. Eludendo la sorveglianza degli insegnanti, attraverso i telefoni cellulari o gli smartphone, dotati di particolari applicazioni e di collegamento a internet, oltre che parlare e scrivere messaggi con i genitori, 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 ai minori, leggere la posta elettronica e comunicare o chattare con sconosciuti, inviare o ricevere messaggi molesti e minacciosi. Eludendo sempre la vigilanza degli insegnanti, gli alunni potrebbero correre gli stessi **rischi** a scuola anche con l'utilizzo dei pc del laboratorio informatico e con un accesso non controllato a internet.

Se da un lato Internet favorisce la libertà di espressione, dall'altra, purtroppo, gli alunni possono farne un uso scorretto, utilizzando il mondo virtuale come ambiente dove mettere in atto atteggiamenti di violenza e prevaricazione. Il fenomeno del ***cyberbullismo***, ossia di «*qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito dei dati personali in danno di minorenni, nonché la diffusione di contenuti online il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo*», ha raggiunto

dimensioni così allarmanti che una legge dello Stato ha recentemente stabilito precise disposizioni a tutela dei minori per prevenirlo e contrastarlo (n. 71/29-05-2017).

Proprio in ottemperanza a tale disposizione legislativa, l'Istituto ha individuato una Referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo. La prima responsabilità del personale della scuola, in primis gli insegnanti, consiste, dunque, nell'imparare a riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente. Tali azioni sono spesso sottovalutate dagli alunni, nonostante la competenza tecnica posseduta. Per arginare il fenomeno del bullismo e del cyber-bullismo occorre soprattutto "gestire", attraverso la sensibilizzazione, le dinamiche devianti di gruppo. In esso gli attori sono tre: il bullo, la vittima e il gruppo. Il gruppo ricopre sempre un ruolo fondamentale perché, anche se in modo passivo o inconsapevole, supporta l'azione del bullo. Nel cyber-bullismo, anche un "*mi piace*" o un "*condividi*" definiscono la posizione del gruppo, in quanto amplificano la portata della violenza nei confronti della vittima. Occorre quindi prestare particolare riguardo alle implicazioni dei comportamenti "pericolosi" attivati o subiti quali:

Ø Sopraffazione fisica, verbale e/o psicologica;

Ø Umiliazione;

Ø Discriminazione;

Ø Aggressività, violenza, molestia attivata o subita;

Ø Isolamento sociale.

In particolare **i rischi** in rete più diffusi sono:

· **Bullismo/Cyberbullismo**: 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:** 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;

L'obiettivo che l'insegnante deve proporsi, dopo avere riconosciuto il pericolo, è agire di conseguenza, con **azioni** di contrasto efficaci e mirate, organizzando per gli alunni momenti di riflessione sui temi dell'utilizzo consapevole di internet e a formandosi su queste tematiche rispetto ai rischi sopra elencati. A tal proposito, la scuola si impegna ad attrezzare le aule con dispositivi elettronici sicuri e protetti e proporrà incontri formativi atti a favorire momenti di riflessione e attività laboratoriali. I genitori si impegneranno a prendere visione della E-Safety Policy e a seguire le azioni promosse dalla scuola per l'utilizzo consapevole della rete. Gli alunni si impegneranno a rispettare i regolamenti e a partecipare attivamente alle occasioni di confronto su queste tematiche organizzate dalla scuola.

Tra le **azioni** utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli alunni in orario scolastico, vi sono le seguenti:

Ø diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web, condividendo materiali messi a disposizione sul sito del progetto "Generazioni connesse";

Ø far rispettare il divieto di utilizzo di dispositivi digitali propri, quali cellulare e smartphone, agli studenti in orario scolastico;

Ø dotare i dispositivi della scuola di filtri che impediscano l'accesso a siti web non adatti ai minori (black list);

Ø bloccare l'accesso a un sito o a un insieme di pagine impedendone la consultazione;

Ø controllare periodicamente i siti visitati dagli alunni;

Ø utilizzare un software in grado di intercettare le richieste di collegamento e di respingere quelle non conformi alle regole stabilite dall'amministratore;

Ø affidare a un gruppo di docenti scelto le regole di filtraggio.

Rilevazione: Che cosa segnalare? Come segnalare? Come gestire le segnalazioni?

Che cosa segnalare?

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 dei social network.

I docenti **segnaleranno** comportamenti inconsueti e inadeguati degli alunni, fatti riferiti dagli alunni e/o dalle famiglie ai docenti; contenuti pericolosi inviati o ricevuti da altri, messi o scaricati in rete dagli alunni.

In particolare si segnaleranno:

Ø contenuti afferenti la violazione della privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, informazioni false, ecc.);

Ø contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, siti d'odio, insulti, ecc…);

Ø contenuti afferenti alla sessualità (messaggi molesti, conversazioni di testo o voce riguardanti la sessualità, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali, ecc…).

Tutte le segnalazioni riportate dai docenti verranno registrate su apposita scheda messa a disposizione dal sito www.generazioniconnesse.it(**Allegato n. 1**).

Come segnalare: quali strumenti e a chi.

Gli insegnanti, anche con l'ausilio tecnico dell'Animatore digitale, possono provvedere a conservare le prove della condotta incauta o scorretta rilevate sui pc della scuola: soprattutto la data e l'ora, il contenuto dei messaggi e, se possibile, l'ID del mittente (es. username, mail, numero di telefono cellulare) o l'indirizzo web del profilo ed il suo contenuto. Per il telefono cellulare ci si può assicurare che l'alunno vittima salvi nel suo telefono ogni messaggio, voce/testo/immagine, conservando così il numero del mittente. Conservare la prova è utile per far conoscere l'accaduto, in base alla gravità, ai genitori degli alunni, al Dirigente scolastico, fino alle autorità competenti. Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno, quantunque riferite a fatti accaduti al di fuori del contesto scolastico, le notizie raccolte sono comunque comunicate ai genitori e al Dirigente scolastico. In particolare, la segnalazione viene fatta a entrambe le famiglie, se oltre alla vittima anche l'autore della condotta negativa è un altro alunno.

Per le segnalazioni di fatti rilevati sono previsti **i seguenti strumenti** che i docenti possono utilizzare sulla base della gravità dell'accaduto:

Ø annotazione del comportamento sul registro e comunicazione scritta ai genitori, che la devono restituire vistata;

Ø convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti;

Ø relazione scritta al Dirigente scolastico.

La legge rimette ai genitori dell'alunno la scelta di richiedere l'ammonizione del colpevole attraverso la querela, per quanto riguarda i reati meno gravi.

Per i reati più gravi, **i docenti hanno l'obbligo di allertare le autorità competenti** e di presentare la denuncia qualora se ne avvisino gli estremi di reato.

Nella denuncia dovrà essere esplicitato:

Ø il fatto e il giorno dell'acquisizione del fatto;

Ø le fonti di prova;

Ø le generalità e il domicilio della persona a cui è attribuito il reato;

Ø la persona offesa;

Ø i testimoni.

A chi bisogna segnalare:

Ø Ai genitori;

Ø Al Dirigente Scolastico;

Ø Al Referente del bullismo e cyberbullismo;

Ø Ai docenti;

Ø Allo psicologo dello Sportello di ascolto dell'I.C.;

Ø Alla helpline di Generazioni Connesse, al numero gratuito 1.96.96.;

Ø Alla Polizia postale.

Inoltre, ci si potrà avvalere dei due servizi messi a disposizione dal Safer Internet Center: il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children. Una volta ricevuta la segnalazione, infatti, gli operatori procederanno a coinvolgere le autorità competenti in materia.

Come gestire le segnalazioni.

Il docente venuto a conoscenza del fatto dovrà:

Ø Informare tempestivamente il Dirigente Scolastico;

Ø Informare tempestivamente la Referente del bullismo e cyberbullismo tramite modulo;

Ø Informare tempestivamente il Coordinatore di classe e il Consiglio di Classe dell'alunno oggetto di cyberbullismo;

Ø Informare i genitori dell'alunno oggetto di cyberbullismo, offrendo loro la possibilità di avere il supporto dello psicologo della scuola per affrontare al meglio la situazione;

Ø La Referente, in collaborazione con il C.d.c. o team docenti, raccoglierà tutte le informazioni possibili;

Ø Il C.d.c. o team docenti valuterà, a seconda della gravità del caso, come sanzionare il/i responsabile/i (qualora sia stato possibile individuarli);

Ø Con la collaborazione dello psicologo della scuola, proporrà agli studenti attività durante le quali questi possano confrontarsi sull'accaduto;

Ø La Referente del bullismo e cyberbullismo, con i docenti coordinatori di classe, si occuperà di tenere un Diario di bordo (**allegato 1**) per monitorare la situazione all'interno dell'Istituto e poter pianificare specifiche azioni preventive;

Ø Il Dirigente valuterà se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali.

Gestione dei casi: definizione delle azioni da intraprendere a seconda della specifica del caso.

Per un'efficace gestione dei casi, i docenti si attengono alle modalità illustrate nello schema messo a disposizione dal sito www.generazioniconnesse.it

Le procedure interne per la rilevazione e la gestione dei casi, nonché la segnalazione alla Dirigenza Scolastica ed eventualmente alle autorità competenti, avvengono secondo i protocolli suggeriti dalla piattaforma messa a disposizione da "Generazioni Connesse", come da schemi allegati:

Allegato n.1: *Schema riepilogativo delle situazioni gestite legate a rischi on-line;*

Allegato n.2: *Schema per la scuola: cosa fare in caso di...cyberbullismo?*

Allegato n.3: *Schema per la scuola: cosa fare in caso di...adescamento on-line/grooming?*

Allegato n.4: *Schema per la scuola: cosa fare in caso di...sexting?*

LINEE GUIDA PER ALUNNI:

· Non comunicare mai a nessuno la tua password e periodicamente cambiala, usando numeri, lettere e 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 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 ri-definizione 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;

· 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:

· 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 comune;

· 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 control" attraverso la sezione sicurezza in internet dal pannello di controllo;

· Attivate il firewall (protezione contro malware) e antivirus;

· Manifestate curiosità: 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;

· Partecipate alle esperienze on-line: navigate insieme a vostro/a figlio/a, incontrate con lui/lei amici on-line, discutete gli eventuali problemi che si presentano;

· 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/a figlio/a a dirvi se vede immagini particolari o se riceve e-mail indesiderate; · Discutete nei dettagli le conseguenze che potranno esserci se vostro/a figlio/a visita deliberatamente siti non adatti, ma non rimproveratelo/a se compie azioni involontarie;

· Spiegate a vostro/a figlio/a 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/a figlio/a che non tutti in Internet sono chi realmente dichiarano di essere;

· Il modo migliore per proteggere i vostri figli è usare Internet con loro, discutere e riconoscere insieme i rischi potenziali.

Il Referente
Ins. Tamara Lazzeretti
Roma, 24 aprile 2018

Il Dirigente Scolastico
Prof. Carmine Giammarini

PATTO BYOD (Bring Your Own Device - Porta il tuo dispositivo)

ALUNNI

Carissimo/a,

come studente/essa della classe … della scuola primaria ".....", avrai la possibilità di poter portare da casa a scuola il tuo device (*dispositivo elettronico*).

Sei un/a bambino/a bravo/a e responsabile e ti meriti questa opportunità **che i tuoi genitori in accordo con i tuoi insegnanti hanno pensato di darti per poter svolgere alcuni lavori a scuola: imparare e divertirti.**

Questa possibilità comprende alcune regole. Leggi bene il seguente contratto. Se non rispetterai queste regole i tuoi genitori ti toglieranno questa possibilità.

1. Il *device* appartiene ai tuoi genitori. Te lo stanno prestando e affidando per un breve periodo di tempo.
2. Appena torni a casa consegna prontamente il tuo *device* a uno dei tuoi genitori che lo spegnerà e/o metterà in carica se c'è bisogno.
3. Il *device* verrà a scuola con te solo quando te lo diranno i tuoi insegnanti.
4. Se il *device* si rompe o svanisce nel nulla, sei responsabile!

Quando sei in rete:

5. Cerca su internet contenuti di cui parleresti anche con i tuoi genitori. Se hai domande rispetto a qualsiasi cosa, chiedi a una persona adulta come mamma e papà e/o ai tuoi insegnanti.
6. Non scrivere qualcosa che non diresti di persona.

E ricorda sempre:

7. Quando sei in compagnia di altre persone puoi anche spegnerlo, non permettere al *device* di trasformarti in una persona maleducata.
8. Gioca a qualche gioco di parole o di logica che stimoli la tua mente, ogni tanto.
9. Tieni gli occhi aperti. Guarda cosa succede intorno a te. Guarda fuori dalla finestra. Ascolta il canto degli uccellini. Fai una passeggiata, fai lavorare la tua immaginazione anche senza *device*.
10. Se userai impropriamente il *device* ti verrà ritirato. Ci metteremo seduti e ne parleremo anche con i tuoi genitori. Ricominceremo da capo. Siamo qui per imparare cose nuove, giorno per giorno, **insieme.**

Speriamo che tu possa essere d'accordo su questi punti. Molte delle "lezioni" che fanno parte della lista non si applicano soltanto al *device*, ma anche alla vita. Fidati della tua testa e del tuo grande cuore, più che di ogni apparecchio.

Se rispetterai queste dieci regole potrai goderti questa nuova favolosa opportunità!

I tuoi insegnanti,

……

Firma dell'alunno/a

Firma del/i genitore/i

DICHIARAZIONIE DEI GENITORI

Il/La sottoscritto/a .....

genitore dell'alunno/a .....

frequentante la classe ...della scuola primaria "....."

DICHIARA

- Di essere al corrente che, in ambito scolastico, i docenti introdurranno, a fianco degli strumenti e dei materiali didattici in uso a scuola, l'utilizzo di applicazioni, contenuti e servizi fruibili in locale e in Internet tramite dispositivi elettronici (*device*) propri;
- Di collaborare con i docenti nel responsabilizzare i ragazzi sulle modalità di accesso a internet e sulle regole a cui attenersi.

AUTORIZZA LA SCUOLA

- A creare un account personale al proprio figlio/a che permette l'accesso alle condivisioni on line e che include strumenti di comunicazioni (posta elettronica, video-chiamate). Lo strumento permette di ricevere ed inviare messaggi e comunicazioni solo con gli altri studenti e con i docenti della scuola.
- Al trattamento dei dati personali del proprio figlio (comprendendo anche fotografie e videoriprese) nella documentazione online delle attività didattiche svolte. L'accesso a queste pubblicazioni sarà consentito esclusivamente agli utenti del dominio della scuola (alunni, famiglie, docenti, dirigente scolastica, uffici).

Data .....

Firma del/i genitore/i

---------- ----------

PATTO BYOD (Bring Your Own Device - Porta il tuo dispositivo)

GENITORI

Il / La sottoscritto/a .....

genitore dell'alunno/a.....

frequentante la classe ... della scuola primaria "....."

AUTORIZZA IL/LA PROPRIO/A FIGLIO/A

- A portare a scuola il proprio dispositivo (specificare marca e modello accanto alla tipologia):
- TABLET .....
- SMARTPHONE .....
- VIDEO-GIOCO MULTIMEDIALE .....
- MICROFONO WIRELESS .....
- ALTRO .....

che sarà usato dallo studente a scuola, in modo individuale o in gruppo, per attività ed esperienze di apprendimento in rete, quali lo scambio e la produzione di materiali condivisi, con la guida e la supervisione dei docenti.

DICHIARA

che durante la permanenza a scuola del dispositivo il proprio figlio sarà responsabile della sua custodia e del suo uso corretto, secondo le regole e le disposizioni concordate con gli insegnanti.

Data .....

firma del/i genitore/i

_____ _____

Allegato 1

Co-financed by the European Union
Connecting Europe Facility

Generazioni Connesse

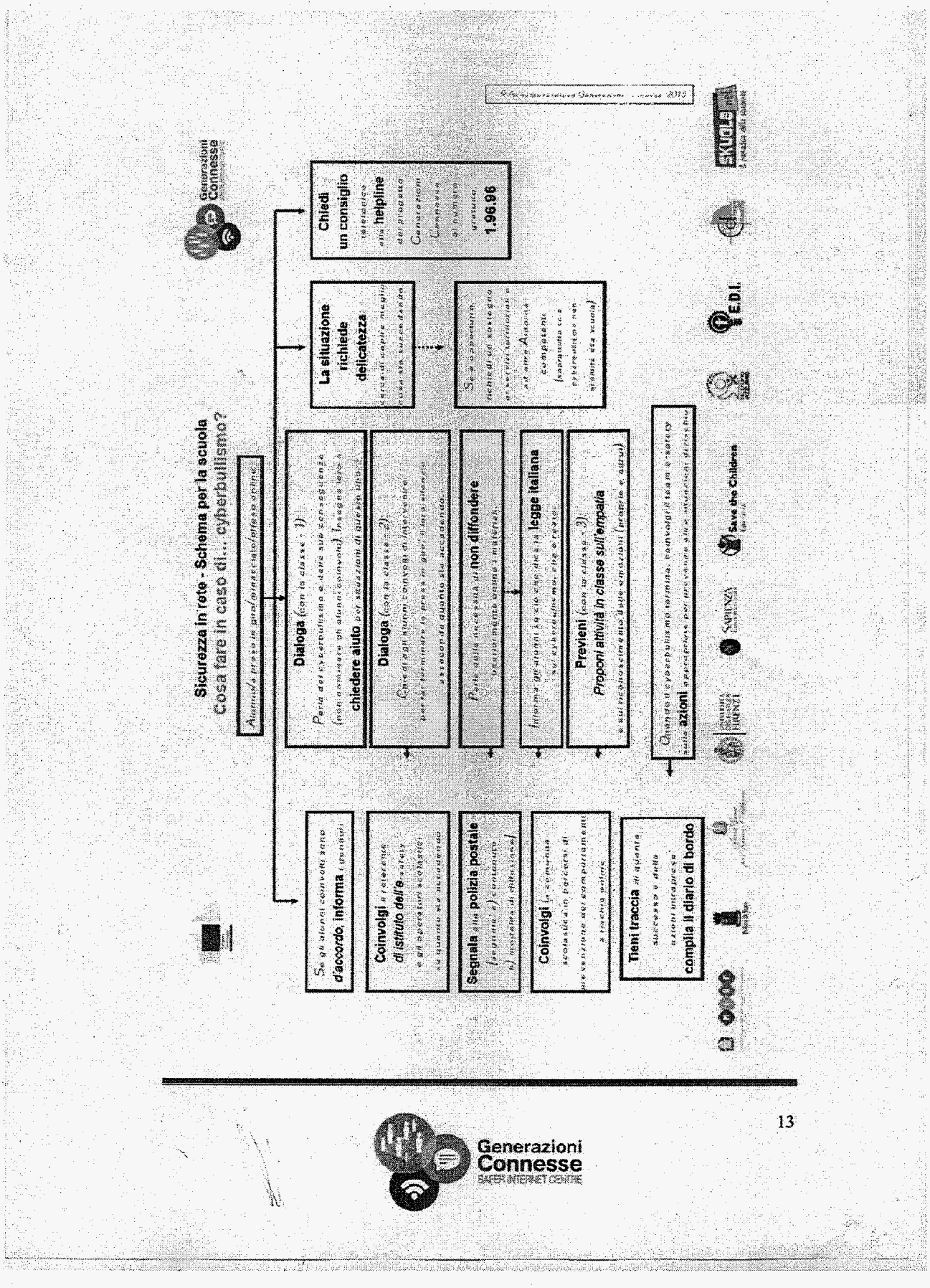
Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi

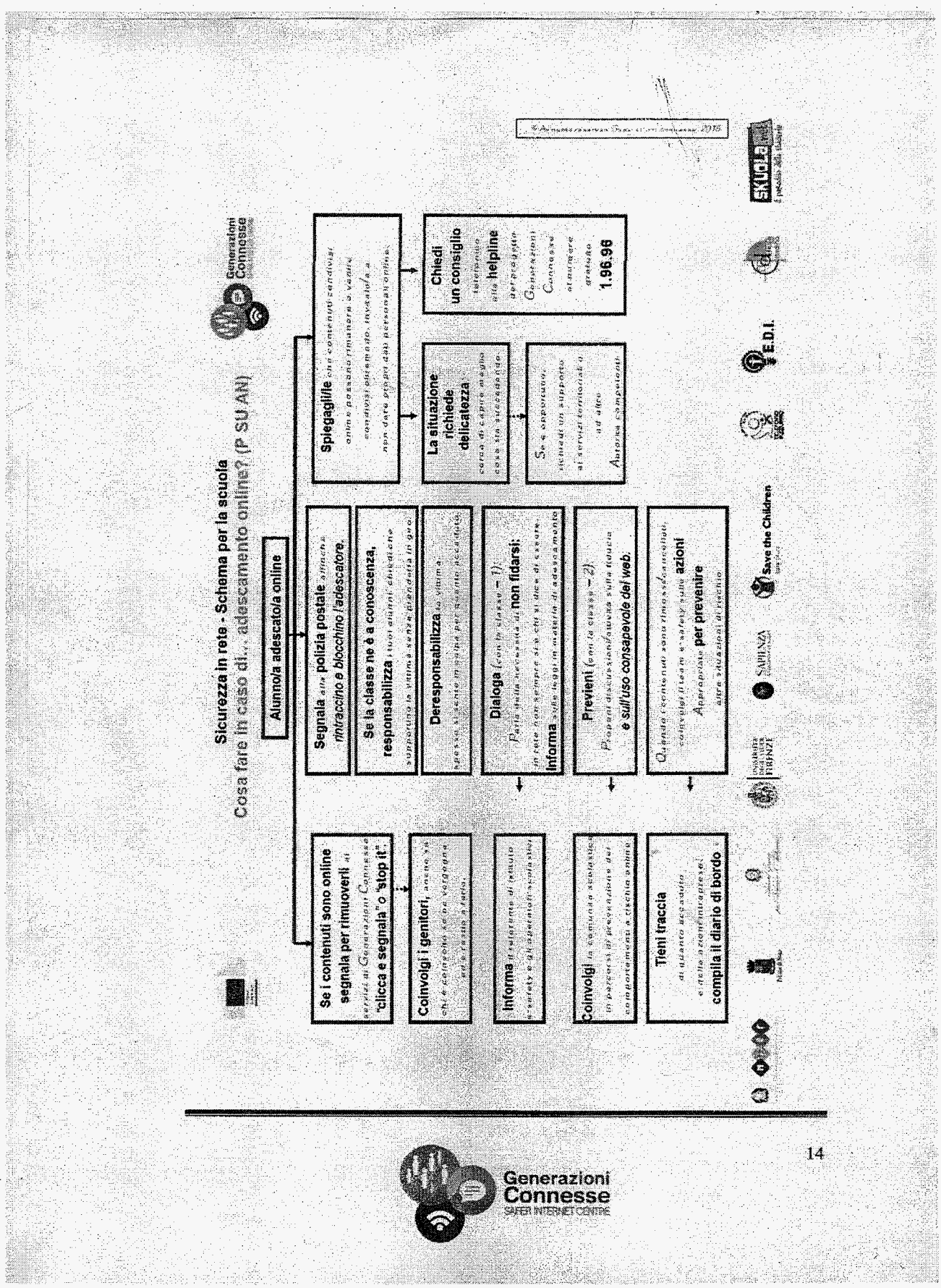
Scuola_____ Anno Scolastico_____

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

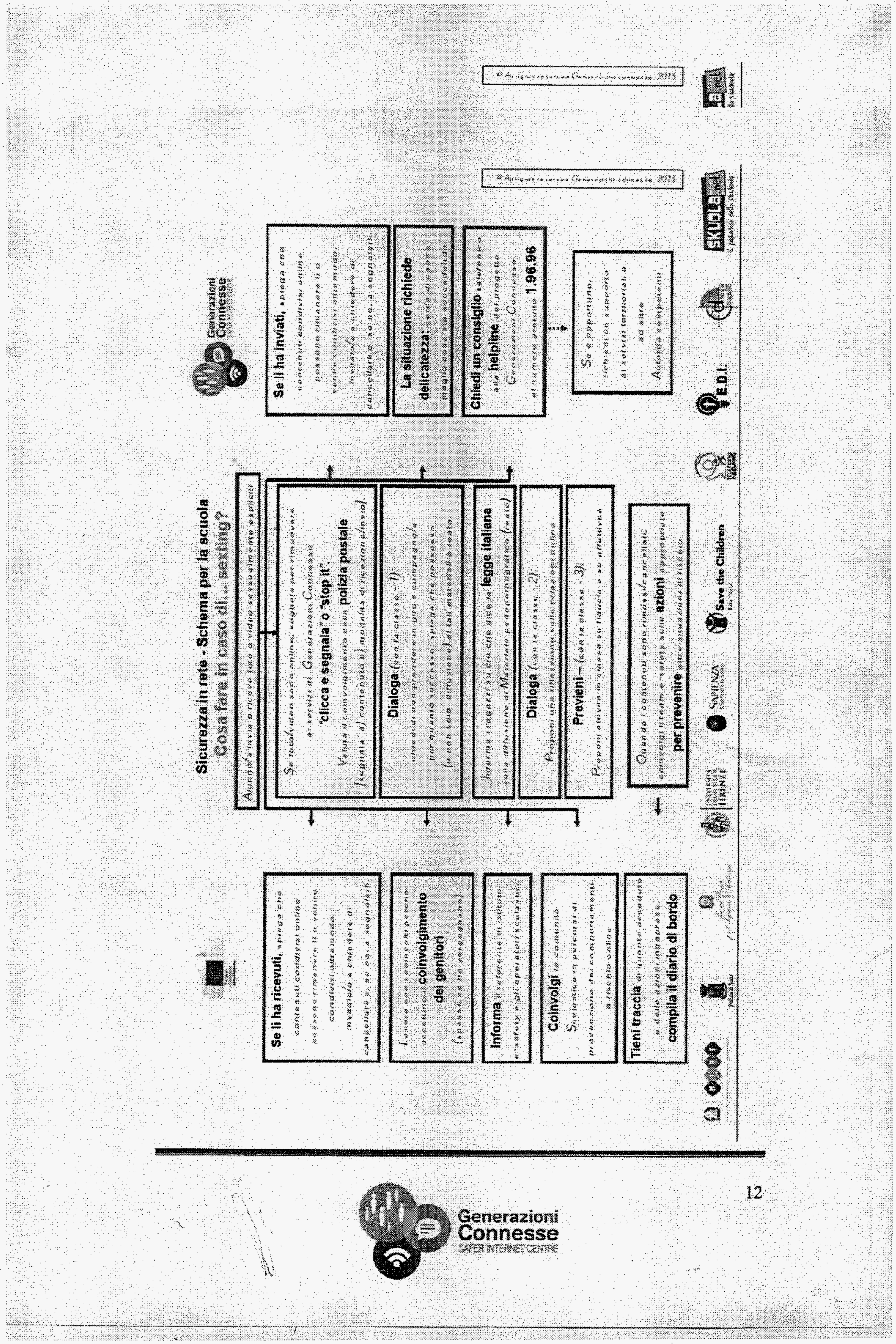
Allegato 2


Sicurezza in rete - Schema per la scuola
Cosa fare in caso di... cyberbullismo?
Dialoga (con la classe - 1)
chiedere aiuto
Dialoga (con la classe - 2)
Previeni (con la classe - 3)
Proponi attività in classe sull'empatia
Coinvolgi
Segnala alla polizia postale
Tieni traccia
compila il diario di bordo
La situazione richiede delicatezza
Chiedi un consiglio
1.96.96
Generazioni Connesse

Allegato 3


Sicurezza in rete - Schema per la scuola
Cosa fare in caso di... adescamento online? (P SU AN)
Generazioni Connesse
Alunno/a adescato/a online
Se i contenuti sono online
segnala per rimuoverli
"clicca e segnala" o "stop it".
Coinvolgi i genitori,
Informa
Coinvolgi
Tieni traccia
compila il diario di bordo
Segnala alla polizia postale
Se la classe ne è a conoscenza,
responsabilizza
Deresponsabilizza
Dialoga
Informa
Previeni
e sull'uso consapevole del web.
per prevenire
Spiegaglielo
Chiedi
un consiglio
helpline
La situazione
richiede
delicatezza
1.96.96
Generazioni
Connesse
SAFER INTERNET CENTRE

Allegato 4


Sicurezza in rete - Schema per la scuola
Cosa fare in caso di... sexting?
Se li ha ricevuti,
coinvolgimento dei genitori
Informa
Coinvolgi
Tieni traccia
compila il diario di bordo
"clicca e segnala" o "stop it".
polizia postale
Dialoga
legge italiana
Dialoga
Previeni –
azioni
per prevenire
Generazioni Connesse
Se li ha inviati,
La situazione richiede delicatezza:
Chiedi un consiglio
helpline
1.96.96
Save the Children
E.D.I.
12
Generazioni Connesse
SAFER INTERNET CENTRE