Generazioni Connesse
SAFER INTERNET CENTRE

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

Co-financed by the European Union
Connecting Europe Facility

POLICY DI e-SAFETY

A.S.2018/2019

Istituto Comprensivo di Villongo

Indice

Indice

CAPITOLO 1

INTRODUZIONE

La Policy di e-Safety è un documento autoprodotto dalla scuola, sulla base dell'indice ragionato messo a disposizione da Generazioni Connesse, sito del progetto Safer Internet Center per l'Italia, volto a descrivere una nuova visione del fenomeno della rete, le norme comportamentali e le procedure per l'utilizzo delle TIC in ambiente scolastico, le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse ad un uso non responsabile delle tecnologie digitali. La policy di e-Safety dell'Istituto Comprensivo di Villongo è un lavoro destinato ad un maggiore approfondimento, per questo potrà essere revisionato annualmente da un gruppo di docenti formato sulle tematiche presenti nella policy.

1.1 SCOPO DELLA POLICY

L'intento del nostro Istituto è quello di promuovere l'uso da parte degli alunni delle tecnologie digitali e di internet in modo responsabile, di far acquisire competenze e corrette norme comportamentali, di prevenire e gestire problematiche che derivano da un utilizzo pericoloso o dannoso delle tecnologie digitali. I nostri allievi dimostrano un'innata predisposizione all'uso delle tecnologie, tuttavia, troppo spesso, a questa abilità si oppone una incapacità, dovuta alla giovane età, di non interpretare bene tutte le informazioni a cui, incessantemente, sono sottoposti, soprattutto attraverso l'uso dei social network. Pertanto la scuola attua parallelamente attività di prevenzione, controllo e formazione di docenti, allievi e famiglie. L'uso delle nuove tecnologie, se non adeguatamente usati, può trasformarsi in una trappola attraverso cui i giovani possono diventare vittime o carnefici di cyberbullismo. Dunque, la policy di e-safety nasce dalla rilevazione di questo bisogno ed è volto a definire:

• norme comportamentali e procedure per l'utilizzo delle tecnologie nell'ambito dell'Istituto;

• misure per la prevenzione e per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

Il Dirigente Scolastico, i docenti, il referente per il bullismo e l'Animatore Digitale hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di internet anche a casa, per prevenire il verificarsi di situazioni pericolose. Per l'elaborazione del presente documento ci si è avvalsi del materiale bibliografico, reperibile in rete e messo a disposizione da Generazioni Connesse.

1.2 RUOLI E RESPONSABILITÀ

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

genitori: devono contribuire, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete; incoraggiare l'impiego delle TIC 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;

Dirigente scolastico: deve garantire la sicurezza (tra cui la sicurezza online) dei membri della comunità scolastica; informare tempestivamente, qualora venga a conoscenza di atti di bullismo/cyberbullismo che non si configurino come reato, i genitori del minore coinvolto (o chi ne esercita la responsabilità genitoriale o i tutori);attivare, nei confronti dello studente che ha commesso atti di bullismo/cyberbullismo, azioni non di carattere punitivo ma educativo; offrire a tutti gli insegnanti una formazione adeguata in merito a un utilizzo positivo e responsabile delle TIC, seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola;

animatore digitale, collaboratore del dirigente e responsabile del laboratorio di informatica: cercano di stimolare la formazione interna all'istituto negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi online e alle misure di prevenzione e gestione degli stessi, monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola, assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione);

Referente bullismo/cyberbullismo: supportare il Dirigente scolastico per la stesura/revisione POLICY DI E-SAFETY; coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.

Direttore dei servizi generali e amministrativi: deve assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni; prevedere interventi di personale tecnico di assistenza per la soluzione di problematiche relative alla rete e all'uso del digitale segnalate dai docenti; 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;

docenti: devono 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; garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi; garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet; 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 abuso, anche sospetto, al Dirigente Scolastico , all'animatore digitale o al referente per il bullismo per le opportune indagini / azioni / sanzioni; non divulgare le credenziali di accesso agli account (username e password) e alla rete wifi; non salvare sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili non protetti; controllare l'uso

delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito); nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei.

Infine, non va sottovalutato il ruolo degli ***studenti*** come primi attori del percorso di acquisizione della capacità di positiva gestione delle proprie competenze digitali: in tale ottica si rende indispensabile coinvolgere anche i più giovani, non solo quali destinatari, ma anche interlocutori attivi e propositivi di tutte le azioni e gli interventi volti alla piena attuazione della Policy. In particolare, il ruolo degli alunni include i seguenti compiti:

• essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;

• avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;

• comprendere l'importanza di adottare buone pratiche di sicurezza online quando si utilizzano le tecnologie digitali per non correre rischi;

• adottare condotte rispettose degli altri anche quando si comunica in rete;

• esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

1.3 CONDIVISIONE E COMUNICAZIONE DELLA POLICY ALL'INTERA COMUNITÀ SCOLASTICA

1. Condivisione e comunicazione della Policy agli alunni:

• all'inizio dell'anno, in occasione dell'illustrazione del regolamento d'istituto agli alunni da parte dei docenti, verrà presentata la policy, insieme ai regolamenti correlati;

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

2. Condivisione e comunicazione della Policy al personale:

• Le norme adottate dalla scuola in materia di sicurezza nell'utilizzo del digitale saranno discusse negli organi collegiali (collegio docenti, riunioni di dipartimento, consigli di classe) 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.

3. 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 TIC saranno organizzati dalla scuola incontri informativi, durante i quali si farà riferimento alla presente policy.

1.4 GESTIONE DELLE INFRAZIONI ALLA POLICY

Tutte le infrazioni alla presente Policy andranno tempestivamente segnalate al Dirigente Scolastico, che avrà cura di convocare le parti interessate onde valutare le possibili azioni da intraprendere.

Circolare: Divieto uso del cellulare a scuola

Il Ministero della Pubblica Istruzione, con la Circolare Ministeriale N° 30/2007,ha stabilito il divieto dell'uso dei telefoni cellulari a scuola, in particolare durante le ore di lezione, ai docenti, alunni e personale di servizio (ATA),in considerazione dei doveri derivanti dal CCNL vigente e dalla necessità di assicurare, all'interno della comunità scolastica, le migliori condizioni per lo svolgimento sereno ed efficace delle attività didattiche, unitamente all'esigenza educativa di offrire ai ragazzi un modello di riferimento esemplare da parte degli adulti.
Sono esonerati dal divieto dell'uso del cellulare soltanto i docenti collaboratori e i docenti responsabili delle sedi che, per motivi logistici ed organizzativi, dovranno essere comunque raggiungibili in qualsiasi momento.

Disciplina del personale scolastico

Le infrazioni in cui è possibile che il personale scolastico incorra nell'utilizzo delle tecnologie digitali e di internet sono:

- utilizzo delle tecnologie e dei servizi della scuola, d'uso comune, non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi; delle tecnologie digitali e di internet;
- vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti.

Per le infrazioni e le relative sanzioni nelle procedure disciplinari vedasi Il Codice disciplinare dei dipendenti pubblici, art.20 disposizioni finali (tabella di raccordo tra le violazioni ai doveri e le sanzioni disciplinari vigenti) Decreto Legislativo 27 ottobre 2009 n. 150; pubblicato sul sito istituzionale.

Disciplina degli alunni

Le 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 considerate sono 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;
- il collegamento a siti web non indicati dai docenti;

Sono previsti pertanto da parte dei docenti provvedimenti "disciplinari" quali:

- richiamo verbale;
- richiamo scritto con annotazione sul diario;
- convocazione dei genitori da parte degli insegnanti;
- convocazione dei genitori da parte del Dirigente scolastico;
- provvedimento di sospensione con eventuali percorsi educativi di recupero anche mediante lo svolgimento di attività riparatorie, di rilevanza sociale o, comunque, orientate verso il perseguimento di un interesse generale della comunità scolastica (quali la pulizia delle aule, piccole manutenzioni, svolgimento di attività di assistenza o di volontariato nell'ambito della comunità scolastica).

Disciplina dei genitori

In considerazione dell'età degli alunni e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC.

Con un'attenzione particolare a:

- la convinzione che se il proprio figlio rimane a casa ad usare il computer sia al sicuro;
- una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio;
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone;
- un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei;

CAPITOLO 2

FORMAZIONE E CURRICULO

Per competenze digitali si intendono competenze che abilitano allo studio, e un domani al lavoro, in maniera aumentata, potenziata, sfruttando le tecnologie per i propri obiettivi, le proprie aspirazioni, i propri interessi personali. Al fine di promuovere la condivisione di buone pratiche per un uso consapevole delle risorse digitali, prevenendo e contrastando "ogni forma di discriminazione e del bullismo, anche informatico" (Legge 107/2015, art. 1, c. 7, l), il nostro Istituto ha aderito al progetto "Generazioni Connesse", coordinato dal MIUR, in partenariato col Ministero dell'Interno-Polizia Postale e delle Comunicazioni e stilerà un Piano d'Azione.

2.1 CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI

La Raccomandazione del Parlamento Europeo e del Consiglio del 18 dicembre 2006 relativa alle competenze chiave per l'apprendimento permanente (2006/962/CE), individua la competenza digitale, ovvero il " saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione." Su queste indicazioni l'Istituto attiverà un percorso sull'uso consapevole delle tecnologie con i seguenti obiettivi:

• promuovere un uso consapevole delle nuove tecnologie;

• sensibilizzare e attivare gli studenti sui rischi e i pericoli derivanti da un uso non corretto dei social network;

• favorire lo sviluppo di una cittadinanza attiva e responsabile;

• educare e sensibilizzare i minori ai rischi associati all'utilizzo di piattaforme di condivisione.

• conoscere e acquisire consapevolezza su natura, ruolo e opportunità delle TSI nel quotidiano;

• distinguere il reale dal virtuale, pur riconoscendone le correlazioni;

• sviluppare le abilità di base nelle TSI (uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni;

• acquisire consapevolezza su come le TSI possono coadiuvare la creatività e l'innovazione;

• riflettere sulle problematiche legate alla validità e all'affidabilità delle informazioni disponibili.

In virtù della valenza trasversale delle competenze digitali, la loro acquisizione verrà promossa attraverso percorsi didattici disciplinari e/o interdisciplinari inerenti diverse aree, coerentemente con gli obiettivi individuati nel curricolo di Istituto.

2.2 FORMAZIONE DOCENTI SULL'UTILIZZO CON SAPEVOLE E SICURO DI INTERNET E DELLE TECNOLOGIE DIGITALI NELLA DIDATTICA

Al fine di promuovere la condivisione di buone pratiche per un uso consapevole e sicuro delle TIC nella didattica, e di prevenire e contrastare "ogni forma di discriminazione e del bullismo, anche informatico" [Legge 170/2015, art. 1, c. 7, l], é necessario organizzare degli incontri con esperti in modalità laboratoriale, in modo che i docenti si trovino nelle stesse condizioni di potenziale rischio nelle quali si potrebbero trovare i loro alunni e imparino quindi le modalità di gestione dei rischi stessi.

2.3 SENSIBILIZZAZIONE DELLE FAMIGLIE

La scuola darà ampia diffusione, tramite pubblicazione sul sito, del presente documento di policy per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e favorire un'attiva collaborazione tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi a un uso non consapevole e critico del digitale. Allo scopo di mantenere viva l'attenzione delle famiglie sull' uso responsabile e sicuro delle nuove tecnologie, l'Istituto promuove opportunità di incontro e formazione per le famiglie sui temi oggetto della Policy, offerte dal territorio, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità.

CAPITOLO 3

GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE TIC DELLA SCUOLA

Accesso a Internet

L'accesso a Internet è possibile nei due plessi della scuola secondaria di I grado e nei tre plessi della scuola primaria sia nei laboratori informatici, presenti in tutti i plessi dell'Istituto comprensivo, sia nelle aule, dotate in parte di LIM con relativo computer portatile custodito in un cassette chiuso a chiave. Nei laboratori di informatica e nelle aule non sono attivi filtri per la navigazione sicura; è invece attivo un software per la gestione e il controllo delle postazioni. Le impostazioni sono definite e manutenute dal responsabile del laboratorio d'informatica ed è in carico a ciascun docente la segnalazione di disservizi.

Gestione accessi (password, backup, ecc.)

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

- amministratore;
- docente;
- alunno.

È possibile effettuare installazioni e aggiornamenti di software solo tramite la password amministratore, fornita al personale di assistenza tecnica e all'Animatore Digitale. E' previsto un backup automatico su server.

E-mail

L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. Le credenziali sono in possesso del personale amministrativo. I docenti utilizzano per scopi didattici il proprio account su dominio istruzione.it. La posta elettronica è protetta da antivirus e da antispam.

Sito web della scuola

La scuola ha un sito web istituzionale https://www.icvillongo.it/ ed è gestito da un responsabile nominato dalla dirigenza.

Social network

Non sono in uso nella nostra istituzione scolastica

Protezione dei dati personali

Il personale scolastico è incaricato del trattamento dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Tutto il personale incaricato riceve poi istruzioni particolareggiate applicabili al

trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi.

In fase di iscrizione degli alunni alla scuola i genitori sottoscrivono un'informativa sul trattamento dei dati personali in ottemperanza degli artt. da 13 a 15 del Regolamento U.E.679/2006**.** All'inizio dell'anno scolastico i genitori rilasciano il consenso all'utilizzo di materiale fotografico e audiovisivo riservato ed elaborati degli alunni per esporli anche in sedi diverse da quelle dell'Istituto quali pubblicazioni in formato digitale e siti WEB.

In caso di utilizzo di piattaforme digitali condivise o di strumenti per la creazione e la gestione di classi virtuali viene acquisito preventivamente il consenso informato dei genitori. In caso di attività di ampliamento dell'offerta formativa, organizzate in collaborazione con Enti esterni, viene richiesto preventivamente ai genitori il consenso informato alle riprese audio/ video e al loro eventuale utilizzo per scopi didattici, informativi e divulgativi anche tramite pubblicazione su siti web. **Responsabile della protezione dei dati** designato ai sensi **dell'art. 37 del Regolamento UE** 2016/679 ("GDPR") è il Sig. Luca Corbellini di AGICOM S.r.l (www.agicomstudio.it),

Come stabilito dalla **circolare del 2007** dell'allora Ministro Fioroni, resta proibito l'uso personale di ogni tipo di dispositivo in classe, durante le lezioni, se non condiviso con i docenti a fini didattici. La violazione di tale dovere comporta, quindi, l'irrogazione delle sanzioni disciplinari

CAPITOLO 4

STRUMENTAZIONE PERSONALE

Per gli studenti: gestione degli strumenti personali - cellulari, tablets, ecc..

Gli alunni della scuola secondaria di primo grado si impegnano a tenere spenti e custoditi in cartella i telefoni cellulari. Nella scuola primaria si chiede alle famiglie di non lasciare i dispositivi ai propri figli. In caso di urgenza per comunicazioni tra gli alunni e le famiglie, su autorizzazione dei docenti e sotto il diretto controllo dei collaboratori scolastici, gli alunni potranno comunicare con le famiglie tramite gli apparecchi telefonici della scuola.

L'uso di dispositivi personali è consentito per lo svolgimento di attività didattiche programmate dai docenti . Gli alunni con certificazione DSA utilizzeranno gli strumenti compensativi quali tablets e computers portatili sotto stretto controllo dei docenti.

Per i docenti: gestione degli strumenti personali - cellulari, tablets, ecc..

Durante le ore di lezione è consentito ai docenti l'uso di dispositivi elettronici personali, come il tablet, unicamente a scopo didattico e a integrazione dei dispositivi scolastici disponibili (il computer di classe), in special modo per l'utilizzo del registro elettronico. E' opportuno che ogni insegnante dia chiare informazioni sul corretto utilizzo della rete; segnali eventuali malfunzionamenti o danneggiamenti al tecnico informatico; non salvi dati personali e sensibili.

Durante il restante orario di servizio l'uso del cellulare è consentito solo per comunicazioni personali che rivestano carattere di urgenza, mentre l'uso di altri dispositivi elettronici personali è permesso per attività funzionali all'insegnamento.

Per il personale della scuola: gestione degli strumenti personali - cellulari, tablets, 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.

Il personale ATA vigila sull'utilizzo non autorizzato delle TIC.

CAPITOLO 5

PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

Rischi

RISCHI	Cyber-bullismo
	Grooming
	Sexting
	Dipendenza da Internet videogiochi, shopping o gambling online,
	Violazione della privacy

I rischi effettivi in cui si può incorrere nell'utilizzo delle TIC a scuola da parte degli alunni derivano da un uso non corretto dei dispositivi elettronici personali e non, collegati ad internet. In particolare i rischi in rete più diffusi sono: Cyberbullismo, Sexting e Grooming.

Azioni di prevenzione

AZIONI	Campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni. I casi possono essere molto variegati, andando dal semplice scherzo di cattivo gusto via sms/Whatsapp a vere e proprie minacce verbali e fisiche, che costituiscono reato. Occorre confrontarsi con il Dirigente Scolastico sulle azioni da intraprendere.
	Sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione. Qualora si venga a conoscenza di casi simili, occorre valutarne la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.
	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione. Verso la componente studentesca: inserimento nel curricolo di temi legati all'affettività, alla sessualità e alle differenze di genere. In casi simili, se l'entità è lieve occorre in primo luogo parlarne con alunne e alunni e rispettivi genitori, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. Manca spesso la consapevolezza, tra ragazzi e adulti, che una foto o un video diffusi in rete divengono di pubblico dominio e la diffusione non è controllabile. In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico
	Informazioni sul fatto che ciò può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito a insaputa di altri) rappresenta un vero e proprio illecito. Divieto per gli alunni di utilizzare propri dispositivi digitali in classe ad eccezione di specifiche e regolamentate attività didattiche
	Informazione sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farle rispettare. Se il comportamento rilevato viola solo le norme di buona convivenza civile e di opportunità, occorre convocare i soggetti interessati per informarli e discutere dell'accaduto e concordare forme costruttive ed educative di riparazione. Qualora il comportamento rappresenti un vero e proprio illecito, il Dirigente Scolastico deve esserne informato in quanto a seconda dell'illecito sono previste sanzioni amministrative o penali.

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.

Che cosa, come rilevare e a chi segnalare

1. Situazioni di disagio
2. Materiale inadeguato: foto "provocanti" inviate ad amici o caricate sul profilo di un Social Network (Sexting) messaggi violenti e offensivi.
3. Comportamenti di bullismo o poco corretti e chiari sia all'interno della scuola, sia al di fuori, soprattutto nel tragitto casa-scuola, scuola-mezzi pubblici.

Rilevazione attraverso:

- **osservazione** sistematica da parte dei docenti nelle classi
- **richieste specifiche** ai ragazzi sul loro benessere all'interno e all'esterno della scuola anche non necessariamente in situazione di palese disagio e ascolto attento di quanto eventualmente raccontano.
- **punto di raccolta segnalazioni di disagio da parte degli alunni** attraverso l'utilizzo di una cassetta in cui inserire delle comunicazioni rivolte ai docenti; essa deve essere posta in un luogo accessibile e controllato da parte del personale ausiliario.

Tale segnalazione non deve assolutamente essere scritta in forma anonima quindi deve contenente nome, cognome, classe, data ed una breve descrizione del fatto che causa disagio.

COME INTERVENIRE:

- **segnalazione del caso** al Coordinatore della classe, al Consiglio di classe
- parlare, ascoltare familiari, insegnanti, amici, servizi del territorio, operatori dell'**HELPLINE** e **HOTLINE**, chiunque sia in contatto con l'alunno/a;
- Gli alunni non sono tutti uguali e non vivono le stesse situazioni, dunque:

a) se l'alunno è seguito, ha alle spalle una famiglia attenta e presente, bisogna coinvolgere oltre al Dirigente Scolastico la famiglia e gli amici;
b) se l'alunno ha poche risorse personali, una famiglia poco presente e non ha una rete di amici, attivare, oltre al Dirigente, una rete extra scolastica di servizi e istituzioni;
c) se l'alunno ha poche risorse personali, una famiglia poco presente ma ha molti amici, coinvolgere, oltre al Dirigente Scolastico, gli amici dell'alunno/a per supportarlo/a; è comunque necessario informare e coinvolgere la famiglia pur nella consapevolezza delle difficoltà che potrebbe avere;
d) se l'alunno ha buone risorse personali ma è solo, instaurare un rapporto diretto e sinergico con l'alunno/a, coinvolgendo il Dirigente scolastico e informando comunque la famiglia

Gestione dei casi

- valutare la necessità di effettuare interventi di osservazione in classe, anche attraverso lo strumento del "diario di bordo"

- pianificare adeguati interventi educativi

- coinvolgere le famiglie in un percorso comune e condiviso di sostegno al disagio. Le azioni poste in essere dalla scuola saranno dirette non solo a supportare le vittime, le famiglie e tutti coloro che sono stati spettatori attivi o passivi di quanto avvenuto, ma anche a realizzare interventi educativi rispetto a quanti abbiano messo in atto comportamenti lesivi, ove si tratti di soggetti interni all'Istituto.

- nei casi di maggiore gravità si valuterà anche il coinvolgimento di attori esterni quali le forze dell'ordine e i servizi sociali, basta la denuncia ad un organo di polizia o all'autorità giudiziaria per attivare un procedimento penale (p.es. lesioni gravi, minaccia grave, molestie); negli altri casi, la denuncia deve contenere la richiesta che si proceda penalmente contro l'autore di reato (querela).

Annessi

1. Procedure operative per la gestione delle infrazioni alla Policy.

- richiamo verbale;
- richiamo scritto con annotazione sul diario;
- convocazione dei genitori da parte degli insegnanti
- convocazione dei genitori da parte del Dirigente scolastico.

2. Procedure operative per la protezione dei dati personali.

Segnalazione e rimozione

Nel caso in cui un minore sia oggetto di atti di cyberbullismo, è prevista la richiesta di oscuramento, rimozione o blocco di qualsiasi dato personale del minore medesimo. La richiesta è effettuata dal minore di quattordici anni o dal genitore o dall'esercente la responsabilità genitoriale e va inoltrata:

✓ al titolare del trattamento
✓ al gestore del sito internet
✓ al gestore del social media

Se i soggetti responsabili non comunicano di aver preso in carico la segnalazione entro 24 ore dal ricevimento della stessa, l'interessato può rivolgersi, mediante segnalazione o reclamo, al Garante per la protezione dei dati personali.

Garante per la protezione dei dati personali.

Il Garante per la protezione dei dati personali ha pubblicato nel sito il **MODELLO per la segnalazione/reclamo in materia di cyberbullismo** *da inviare a:* **cyberbullismo@gpdp.it.** Il Garante provvede entro quarantotto ore dal ricevimento della richiesta.

- Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni;

- Polizia di Stato – Questura o Commissariato di P.S. del territorio di competenza;
- Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza
- Polizia di Stato – Commissariato on line (attraverso il portale http:// www.commissariatodips.it).

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

Le scuole possono inoltre segnalare episodi di cyberbullismo e la presenza di materiale pedopornografico on line:

- al servizio **Helpline di Telefono Azzurro 1.96.96**, con una piattaforma integrata che si avvale di telefono, chat, sms, whatsapp e skype - strumenti per aiutare i ragazzi e le ragazze a comunicare il proprio disagio;
- alla **Hotline "Stop-It**" di **Save the Children**, all'indirizzo **www.stop-it.it**, che consente agli utenti della Rete di segnalare la presenza di materiale pedopornografico online. Attraverso procedure concordate, le segnalazioni sono successivamente trasmesse al Centro Nazionale per il Contrasto alla Pedopornografia su Internet, istituito presso la Polizia Postale e delle Comunicazioni, per consentire le attività di investigazione necessarie.

4. Procedure operative per la gestione dei casi.

- tenere traccia di quando accade, della tipologia di interventi, degli esiti; **(vedi diario di bordo allegato 2);**

- a scuola deve essere presente un apposito modulo per le segnalazioni **(vedi allegato 3);**

5. Protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi.

- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Corecom (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale:** supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di internet.
- **Polizia Postale e delle Comunicazion**i: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune ragioni, come il Lazio, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da internet ed alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico:** segnalano all'Autorità Giudiziaria i Servizi sociali e competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio di tali

- **Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza.

CAPITOLO 6

AZIONI

L'obiettivo che l'insegnante deve proporsi dopo avere riconosciuto il pericolo è agire di conseguenza, con azioni di contrasto efficaci e mirate, rispetto ai rischi sopra elencati. Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli studenti in orario scolastico, vi sono le seguenti:

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

• richiedere di volta in volta autorizzazione esplicita da parte dei genitori all'utilizzo dei dati personali degli alunni (es. liberatoria per la pubblicazione di foto, immagini, video relativi al proprio/a figlio/a per la partecipazione a progetti didattici e altro);

• far rispettare il divieto di utilizzo di dispositivi digitali propri, quali cellulare, agli studenti in orario scolastico. Le dovute eccezioni (uso del cellulare per comunicazioni alunno-famiglia in occasione di uscite didattiche) andranno espressamente regolamentate e dovranno comunque avvenire sotto la supervisione diretta di un docente responsabile;

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

Azioni utili a impedire un utilizzo incauto, scorretto o criminoso degli strumenti digitali - materiali inviati, scaricati, ricevuti o condivisi - su dispositivi digitali in uso a scuola (principalmente pc) sono:

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

• controllare periodicamente i siti visitati dagli alunni;

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

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

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;
- Qualora necessario puoi utilizzare " **You Pol"** , una nuova **mobile app** sviluppata dalla Polizia di Stato, diretta alla creazione di un canale di comunicazione privilegiato per la segnalazione, in modo semplice ed immediato, di episodi di bullismo, maltrattamenti e spaccio di stupefacenti, anche in forma anonima.
- 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, dell' 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 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 (sportello di ascolto psicologico, 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 il Dirigente Scolastico, l'Animatore digitale, il Referente per il bullismo per un eventuale denuncia 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 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;
- 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, di approfondimenti disciplinare…
- Partecipa alle esperienze on-line: naviga insieme a tuo figlio, 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 riconoscerne insieme i rischi potenziali.

Allegati:
all. 1 Scheda di segnalazione
all. 2 Esempio di Diario di bordo per il monitoraggio delle situazioni a rischio
all. 3 Sintesi degli articoli del Codice Penale e Civile inerenti i reati ascrivibili al cyberbullismo

Allegato. 1 MODULO PER LA SEGNALAZIONE DI CASI

<table>
<tr><td colspan="2">Nome di chi compila la segnalazione: Ruolo:

Data: Scuola:</td></tr>
<tr><td>Descrizione dell’episodio o del problema</td><td></td></tr>
<tr><td>Soggetti coinvolti</td><td>Vittima/e Classe

Bullo/i Classe</td></tr>
<tr><td>Chi ha riferito l’episodio?</td><td>La vittima

Un compagno della vittima: nome

Genitore: nome

Insegnante:Nome

Altri, specificare</td></tr>
</table>

Atteggiamento del gruppo	Da quanti compagni è sostenuto il bullo Quanti compagni supportano la vittima o potrebbero farlo
Gli insegnanti sono intervenuti in qualche modo?	
La famiglia o altri adulti hanno cercato di intervenire?	
Chi è stato informato della situazione?	○ Coordinatore di classe data: ○ Consiglio di classe data: ○ Dirigente Scolasico data: ○ La famiglia della/e vittima/e data: ○ La famiglia del/i bullo/i data: ○ Le forze dell'ordine data: ○ Altro, specificare

Co-financed by the European Union
Connecting Europe Facility

Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi

Scuola_____ Anno Scolastico_____

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

Allegato 3

Articoli inerenti il bullismo/cyberbullismo

Chi compie atti di bullismo e cyberbullismo è responsabile di reati penali e danni civili. I ragazzi e le ragazze che fanno azioni di bullismo possono commettere reati. Secondo il codice penale italiano i comportamenti penalmente rilevanti in questi casi sono:

percosse	art. 581
lesione personale	art. 582
ingiuria	art. 594
diffamazione	art. 595
violenza privata	art. 610
minaccia e,molestie atti persecutori/stalking	art. 612 art. 612 bis
danneggiamento	art. 635
produzione,detenzione e cessione di materiale pedopornografico	art.600 bis
reati contro la privacy	Violazione legge 547/93

Normative di riferimento

Protezione dati personali art. 13 D.Lgs 30 giugno 2013 , n. 196 , artt. dal 13 al 15 Regolamento U.E 679/2006

Legge 29 maggio 2017, n. 71. Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo. (17G00085) (GU Serie Generale n.127 del 03-06-2017). note: Entrata in vigore del provvedimento: 18/06/2017 ...

Direttiva Ministeriale 5 febbraio 2007, **n.16**. Oggetto: linee di indirizzo generali ed azioni a livello nazionale per la prevenzione e la lotta al bullismo.

Direttiva Ministeriale del 15 marzo 2007 - Linee di indirizzo utilizzo telefoni cellulari

Linee di orientamento per azioni di prevenzione e contrasto al bullismo e al cyberbullismo (13 aprile 2015)