POLICY DI E-SAFETY

A.S.2017/2018

Istituto comprensivo “E. Donadoni”

INDICE RAGIONATO

E-Safety Policy

1. Introduzione

- Scopo della Policy.
- Ruoli e Responsabilità (*che cosa ci si aspetta da tutti gli attori della Comunità Scolastica*).
- Condivisione e comunicazione della Policy all'intera comunità scolastica.
- Gestione delle infrazioni alla Policy.
- Monitoraggio dell'implementazione della Policy e suo aggiornamento.
- Integrazione della Policy con Regolamenti esistenti.

2. Formazione e Curricolo

- Curricolo sulle competenze digitali per gli studenti.
- Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica.
- Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
- Sensibilizzazione delle famiglie.

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

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

4. Strumentazione personale

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

5. Prevenzione, rilevazione e gestione dei casi

Prevenzione

- Rischi
- Azioni

Rilevazione

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

Gestione dei casi

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

Annessi

1. Procedure operative per la gestione delle infrazioni alla Policy.
2. Procedure operative per la protezione dei dati personali.
3. Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni.
4. Procedure operative per la gestione dei casi.
5. Protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi.

1. INTRODUZIONE

1.1 Scopo della Policy

L'istituto Donadoni, nell'ambito dell'iniziativa "Generazioni connesse" (Safer Internet Centre Italy III), progetto promosso dal Miur, finanziato dalla Commissione Europea, ha redatto un documento con l'obiettivo di educare e sensibilizzare gli insegnanti, gli studenti e i genitori all'uso sicuro e consapevole di internet. Il presente documento vuole descrivere in maniera chiara ed esaustiva le linee guida dell'istituto in materia di:

- utilizzo consapevole delle TIC (Tecnologie dell'informazione della comunicazione) nella didattica e negli ambienti scolastici;
- prevenzione/gestione di situazioni problematiche relative all'uso delle tecnologie digitali.

Inoltre il progetto "Generazioni connesse" è stato inserito nel nostro Piano Triennale dell'Offerta Formativa e le azioni preventivate nel Piano d'Azione della nostra scuola.
Le attività di promozione all'utilizzo delle tecnologie digitali nella didattica costituiscono un tema centrale per l'attuazione del Piano Nazionale Scuola Digitale. Il lavoro per la realizzazione del documento di E-Safety si integra con la redazione del Piano di Miglioramento dell'Istituto sulle nuove tecnologie.

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

Dirigente scolastico:

- presentare e divulgare la Policy all'attenzione al Collegio dei Docenti e del Consiglio di Istituto;
- 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;
- garantire, come suddetto, l'informazione delle iniziative intraprese e delle attività svolte.
- attivare specifiche intese con i servizi territoriali (servizi della salute, servizi sociali, forze dell'ordine, servizi minorili dell'amministrazione della Giustizia) in grado di fornire supporto specializzato e continuativo ai minori coinvolti ove la scuola non disponga di adeguate risorse;
- al dirigente scolastico e al docente referente non sono attribuite nuove responsabilità o ulteriori compiti, se non quelli di raccogliere e diffondere le buone pratiche educative,

- controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola.

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.

Animatore digitale

- stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".

Direttore dei Servizi Generali e Amministrativi:

- assicurare 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;
- garantire il funzionamento dei diversi canali di comunicazione della scuola (circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni;
- notificare documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.

Docenti:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- guidare la navigazione di studentesse e studenti, nelle lezioni in cui l'uso di Internet è pianificato, verso siti controllati come idonei per il loro uso, onde evitare di incontrare materiali inadatti;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'animatore digitale 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;
- proporre agli alunni attività di ricerca di informazioni in rete fornendo opportunamente loro indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento.

- usare in modo corretto i sistemi informatici e la tecnologia digitale in accordo con i termini previsti da questa policy
- non utilizzare dispositivi personali durante le attività didattiche se non espressamente consentito dal personale docente;
- avere una buona comprensione delle possibilità di ricerca sul web e della necessità di evitare il plagio, rispettare le normative sul diritto d'autore, non diffondere dati personali;
- comprendere l'importanza della segnalazione di ogni abuso, uso improprio o accesso a materiali inappropriati e conoscere il protocollo per tali segnalazioni;
- conoscere e comprendere le politiche sull'uso di dispositivi mobili e di macchine fotografiche digitali;
- capire le politiche di utilizzo delle immagini ed essere consapevoli del significato e della gravità del cyber-bullismo;
- capire l'importanza di adottare buone pratiche di sicurezza informatica in tutti i momenti della vita, a tutela dell'incolumità propria e altrui e per evitare di perpetrare reati punibili sia a livello scolastico sia da parte della magistratura.

Genitori:

- sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;
- seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di internet;
- concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet;
- fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e dei relativi device in generale;
- 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.

1.3 Condivisione e comunicazione della Policy all'intera comunità scolastica

La policy è stata redatta dalla commissione bullismo/cyberbullismo, da un gruppo di docenti che hanno partecipato all'intervento formativo del progetto 'Generazioni Connesse' il 18 dicembre 2017 , e condivisa dall'animatore digitale e dal tecnico informatico.
Sarà inserita all'interno del Piano Triennale dell'Offerta Formativa, un documento pubblico, consultabile alle famiglie nel sito della scuola alla pagina:
http://www.istitutodonadoni.it/index.php/il-pof

a) **Condivisione e comunicazione della Policy al personale scolastico**
- le norme adottate dalla scuola in materia di sicurezza nell'utilizzo del digitale saranno rese note tramite pubblicazione del presente documento sul sito web della scuola.

b) **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 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.

c) **Condivisione e comunicazione della Policy agli alunni**
- attraverso la condivisione del patto educativo di corresponsabilità, attività, laboratori, incontri, spettacoli che portino a riflettere su rischi e opportunità del web.

1.4 Gestione delle infrazioni alla Policy

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;
- 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;
- un utilizzo del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria indirizzi o contenuti non idonei.

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

1.5 Monitoraggio dell'implementazione della Policy e suo aggiornamento

Il presente documento potrà essere aggiornato, migliorato annualmente.

1.6 Integrazione della Policy con Regolamenti esistenti

La Policy è coerente con quanto stabilito nei Regolamenti vigenti.

2.Formazione e Curricolo

Attualmente non esiste nell'Istituto un curricolo specifico sulle competenze digitali. Quest'ultime sono però declinate nel documento delle competenze europee e vengono promosse in maniera trasversale dai docenti, sulla base delle loro pratiche di insegnamento. All'interno di un curricolo verticale esistente, l'istituto svilupperà uno specifico curricolo finalizzato all'acquisizione di competenze digitali per gli studenti. (Potrà essere fatto se e quando tutte le sedi saranno provviste di connessione e strumenti digitali)

2.1 Formazione e Curricolo Curricolo sulle competenze digitali per gli studenti

Al termine della scuola primaria e al termine del primo ciclo di istruzione le competenze digitali vengono certificate sulla base dei seguenti profili.

• **Primaria**: usa le tecnologie in contesti comunicativi concreti per ricercare dati e informazioni e per interagire con soggetti diversi;

• **Secondaria di primo grado**: usa con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo.

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

La figura dell'Animatore Digitale insieme al team avrà il compito di promuovere la didattica multimediale.

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

E '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.

2.4 Sensibilizzazione delle famiglie

La Policy verrà integrata nel Patto di Corresponsabilità Educativa sottoscritta dai docenti e dai genitori e condivisa con gli alunni all'inizio dell'anno scolastico.

3 Gestione dell'infrastruttura e della strumentazione ICT della scuola

3.1 Accesso ad internet: filtri antivirus e sulla navigazione.

3.2 Gestione accessi (password, backup, ecc.).

Primaria Locatelli e Ghisleni: le classi sono dotate di pc connessi alla rete wifi e/o cablata. L'aula di informatica è dotata di pc connessi a internet tramite la rete cablata e accessibili con un unico nome utente e password. I pc delle aule a tutela dei dati sensibili, sono dotate di user e password propria conosciute dall'equipe pedagogica e dal tecnico di istituto.

Secondaria succursale: tutte le aule curriculari sono dotate di pc portatili accessibili tramite password e connessi alla rete cablata e/o wifi.

Secondaria sede: tutte le aule curriculari sono dotate di pc portatili accessibili tramite password e connessi alla rete cablata. Le aule adibite a laboratorio possono usufruire di un pc portatile di uso comune, attualmente non utilizzabile con internet poiché l'aula in questione non è cablata.

3.3 E-mail.
L'account di posta elettronica è solo quello istituzionale, utilizzato dagli uffici amministrativi, sia per la posta in ingresso che in uscita. Le credenziali sono in possesso del personale amministrativo.

3.4 Blog e sito web della scuola

Il sito istituzionale della scuola http://www.istitutodonadoni.it/ è attivo e gestito da un responsabile nominato dal dirigente.

3.5 Social network.

Non vengono utilizzate piattaforme digitali per il momento;

3.6 Protezione dei dati personali.

In fase di iscrizione degli alunni alla scuola i genitori sottoscrivono un'informativa sul trattamento dei dati personali in ottemperanza **all'art. 13 D.Lgs 30 giugno 2013 , n. 196**.
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 **Dott. Giancarlo Favero di Data Security (**www.datasecurity.it), divisione sicurezza di Swisstech S.r.l (contatti: giancarlo.favero@datasecurity.it/link
forum: http://forum.enti.it/viewforum.php?f=3**)**.

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.

4.1 Per gli studenti: è vietato l'utilizzo di cellulari per l'intera durata delle attività scolastiche (intervalli inclusi). Alunni con Bisogni Educativi Speciali potranno utilizzare il proprio notebook o tablet e la connessione wifi della scuola. E'consentito a tutti gli alunni in casi specifici concordati con il docente (uso di e-book, uscite didattiche, produzioni multimediali) l'utilizzo di dispostivi elettronici personali per scopi didattici (BYOD).

4.2 Per i docenti: durante il loro orario di servizio è consentito l'utilizzo di dispostivi elettronici personali solo ed esclusivamente per fini didattici.

4.3 Per il personale della scuola: è vietato l'utilizzo di personal device durante l'orario di servizio.

5.Prevenzione, rilevazione e gestione dei casi

5.1 Prevenzione: rischi e azioni

La diffusione delle tecnologie digitali e dell'accesso a Internet presso i più giovani sta portando profondi **cambiamenti nelle dinamiche relazionali e in quelle identitarie**, trasformando linguaggi, modalità di comunicazione, abitudini e stili di vita e offrendo inedite potenzialità di crescita. Se, dunque, le Tecnologie dell'Informazione e della Comunicazione (TIC) sono parte integrante della vita quotidiana dei più giovani, in quanto strumenti privilegiati di comunicazione e di relazione, ma anche di informazione, studio, creatività e partecipazione, esse pongono però delle **questioni associate alla "sicurezza" e al comportamento sociale**. Non bisogna infatti cadere nello stereotipo di una categoria uniforme di bambini/e e adolescenti "competenti", sollevando gli adulti dal proprio **ruolo educativo e dalla responsabilità** di promuovere presso i più giovani un **uso consapevole** e quindi anche un **uso integrativo** (e non sostitutivo) delle tecnologie digitali. Siamo di fronte ad una realtà complessa, pensata prevalentemente per un mondo adulto e nella quale trovano spazio contenuti e comportamenti potenzialmente dannosi.
I **rischi online** rappresentano tutte quelle situazioni problematiche derivanti da un uso non consapevole e non responsabile delle tecnologie digitali da parte di bambini/e, ragazzi e ragazze

quali:

RISCHI	AZIONI
Adescamento online (grooming)	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.

Cyberbullismo	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.
Dipendenza da Internet videogiochi, shopping o gambling online,	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.
Esposizione a contenuti pornografici, violenti, razzisti	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione e sensibilizzazione sulla necessità di monitorare l'esperienza online dei propri figli. Verso la componente studentesca: inserimento nel curricolo di temi legati alla affidabilità delle fonti online, all'interculturalità e al rispetto delle diversità. Qualora si venga a conoscenza di casi simili, occorre convocare i genitori per invitarli a un maggiore controllo sulla fruizione di internet da parte dei propri figli e/o sulla necessità di non usufruirne in presenza degli stessi.
Sexting e pedopornografia.	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
Violazione della privacy	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.

5.3 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.

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

Nome di chi compila la segnalazione:	Ruolo:
Data:	Scuola:

Descrizione dell'episodio o del problema	

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

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?		

Generazioni Connesse
SAFER INTERNET CENTRE

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

Co-financed by the European Union
Connecting Europe Facility

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
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)