ISTITUTO COMPRENSIVO "NINO CORTESE"
CASORIA (NA)

E-Safety Policy

ANNO SCOLASTICO 2017/2018

Sommario

1. Introduzione

1.1 - Premessa

Il curricolo del nostro istituto prevede, in ottemperanza alla *Raccomandazione europea del 2006 per il Lifelong Learning*, alle *Indicazioni Nazionali per il curricolo*, alla *Legge 107/2015* e al *P.N.S.D.*, che gli studenti e le studentesse acquisiscano le competenze digitali, saperi chiave per vivere attivamente nella nostra società dell'informazione. Ma, poiché le aree delle competenze digitali, oltre all'informazione, alla comunicazione e alla creazione di contenuti, includono anche la sicurezza, ritiene di dover abbracciare, in un'ottica pedagogica, oltre alla dimensione più strettamente tecnologica, anche la dimensione cognitiva (per la valutazione critica degli strumenti e dei contenuti digitali) ed etica (per l'interazione corretta e responsabile nel mondo del digitale).
Il nostro istituto si propone, dunque, oltre che di accrescere la formazione e l'aggiornamento di docenti e discenti sull'uso delle tecnologie nel processo di insegnamento-apprendimento, anche di sviluppare in tutta la comunità scolastica la consapevolezza e l'appropriatezza di quest'uso a scuola e all'esterno, conscio di essere oggi chiamato dalla nuova normativa (in particolare dalla *Legge 71/2017*, dalle *Linee di orientamento per la prevenzione e il contrasto del Cyberbullismo-Ottobre 2017* e dal *Piano Nazionale per l'educazione al rispetto*), in collaborazione con le famiglie, con le Forze di Polizia e con i servizi socio-territoriali, a mettere in campo strumenti che consentano di rilevare circostanze potenzialmente pericolose (in particolare, se legate proprio alla frequenza della scuola) e a prevenire, contrastare, gestire e monitorare le situazioni di rischio e disagio derivanti da un uso inappropriato e non abbastanza sicuro delle nuove tecnologie.
Ciò ha reso necessaria una riflessione profonda, anche in ragione di un cambiamento radicale rispetto al passato: l'onnipresenza dei moderni dispositivi portatili, uniti al richiamo dei social media, che stanno avendo un impatto epocale sul modo in cui studenti e studentesse si informano, comunicano e trascorrono il tempo libero.
Da questa riflessione e dagli scambi della dirigenza e dei docenti con gli studenti e le studentesse, con i genitori e con tutto il personale scolastico (avvenuti, in particolare, durante i seminari con un esperto di *Telefono Azzurro*), è derivata la e-safety policy riportata in questo documento, la cui struttura e i cui approfondimenti tematici sono frutto della consultazione di corsi e materiali reperibili sul sito del progetto, coordinato dal Miur, "*Generazioni Connesse*" (www.generazioniconnesse.it), a cui questa scuola ha aderito.
Il documento si integra con gli obiettivi di miglioramento riguardanti la dotazione e la formazione tecnologica della scuola ed è costituito dai principi fondamentali condivisi riguardanti l'uso delle TIC, dalle buone pratiche, dai regolamenti e dalle misure di prevenzione e di intervento della scuola.

1.2 - Scopo della Policy

Il documento di e-policy ha un carattere programmatico, in quanto in esso confluiscono organicamente le linee guida adottate dal nostro istituto sulle nuove tecnologie. Esso conferma gli obiettivi del piano digitale incluso nel PTOF, teso precipuamente ad accrescere e a migliorare le dotazioni hardware e software della scuola (anche rendendole più sicure) e le competenze tecnologiche di docenti, discenti e di tutto il personale scolastico. Questi obiettivi vengono tuttavia integrati in una condotta digitale sempre più riflessiva, che, investendo il processo di insegnamento-apprendimento e l'intera vita scolastica, intende rendere i membri della nostra comunità di studio più consapevoli dei fattori in gioco nelle varie attività con i media, sia come "lettori" che come "scrittori".
Le linee di intervento, in questo senso, includono:

- la definizione attenta e partecipata dell'approccio della scuola alle tematiche legate alle competenze digitali, alla sicurezza online e a un uso positivo delle TIC nella didattica;
- le norme comportamentali e le procedure per l'utilizzo delle TIC in ambiente scolastico;

- le misure di prevenzione, rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

In quanto programmatica, la e-policy è passibile di modifiche e ampliamenti, in base ai cambiamenti che interverranno nel mondo del digitale e nella nostra scuola e a quanto indicato dal Miur, dall'Unione Europea e dal *Progetto Generazioni Connesse (SIC Italy)*, nell'ambito del programma *The Connecting Europe Facility (CEF)*.

1.3 - Ruoli e Responsabilità

Il ***Dirigente Scolastico*** assicura al personale una formazione adeguata per svolgere i ruoli legati alla sicurezza online e attiva specifiche intese con i servizi territoriali, in grado di fornire formazione agli studenti e alle studentesse della scuola e supporto ai minori coinvolti nei casi di disagi legati all'uso non adeguato del web (e, in particolare, nei casi di cyberbullismo), informandone tempestivamente le famiglie. Egli ha un ruolo di primo piano nello stabilire le linee guida contenute nella e-policy ed è responsabile e garante della sua applicazione.

L'***Animatore Digitale e il docente referente per il cyberbullismo*** promuovono e coordinano le attività di formazione sulle competenze digitali, elaborano e pubblicano la e-policy sul sito della scuola, definendo tutte le misure di sicurezza informatica, ne diffondono i contenuti in tutta la comunità scolastica e controllano la sua applicazione, coordinano le azioni di prevenzione, rilevazione e contrasto delle problematiche legate a un uso poco sicuro della Rete (con particolare attenzione alle attività di prevenzione di forme di esclusione e discriminazione e agli atti di bullismo e cyberbullismo).

Il ***DSGA*** assicura, nei limiti delle risorse disponibili, gli interventi tecnici per garantire che l'infrastruttura tecnologica e i canali di comunicazione digitali siano funzionanti e sicuri.

I ***Docenti*** si informano e si aggiornano sull'uso e sulle problematiche attinenti l'uso delle nuove tecnologie; inseriscono tematiche legate alla sicurezza online e al contrasto agli stereotipi e alle discriminazioni nelle attività di insegnamento-apprendimento; guidano e supervisionano gli studenti e le studentesse durante le lezioni che prevedono l'utilizzo di Internet e segnalano le problematiche rilevate durante la navigazione in Rete.

Il ***Personale scolastico*** conosce e promuove la politica di e-safety della scuola, monitora l'uso dei dispositivi portatili e non, e segnala abusi sospetti e problematiche. Controlla che le comunicazioni degli studenti e delle studentesse all'interno della scuola avvengano solo attraverso i sistemi scolastici.

I ***Genitori*** sostengono la scuola nel promuovere la sicurezza online, leggendo la e-policy e partecipando agli incontri organizzati dalla scuola sulle tematiche relative alla sicurezza online. Seguono gli studenti e le studentesse nello studio a casa, adottando linee di intervento e regole d'uso dei dispositivi digitali coerenti con quelle della scuola.

Gli ***Studenti*** si impegnano a comprendere e ad applicare la e-policy della scuola, nonché a segnalare abusi e usi impropri. Intraprendono le azioni attese e loro indicate se loro stessi o un compagno o una compagna sono in situazioni a rischio online. Applicano i regolamenti (quelli generali e quelli specifici delle aule di informatica) e le pratiche della scuola sulla sicurezza online.

1.4 - Condivisione e comunicazione della Policy all'intera comunità scolastica.

Poiché la e-policy si applica a tutta la comunità scolastica, una volta approvata in via definitiva dal Collegio Docenti e dal Consiglio d'Istituto, viene condivisa con tutti i suoi membri mediante pubblicazione sul sito della scuola.

Un'adeguata formazione/informazione, oltre che mediante il presente documento, sarà garantita mediante il link al sito www.generazioniconnesse.it e nella sezione Osservatorio Cyberbullismo sul sito della scuola.

Tutto il personale scolastico, inoltre, sarà reso consapevole che il traffico in Rete potrebbe essere monitorato e che il sistema di filtraggio e monitoraggio è supervisionato dalle funzioni strumentali dell'area 4 (Gestione risorse tecnologiche e informatiche).
L'accordo di utilizzo con le famiglie verrà siglato all'inizio del primo anno, all'interno del **Patto Educativo di Corresponsabilità** loro rilasciato. La collaborazione con esse nel perseguire la sicurezza nell'uso delle TIC sarà in seguito costantemente incoraggiata, in occasione degli **incontri scuola-famiglia, collegiali, assembleari e individuali.**
I docenti provvederanno all'istruzione degli studenti e delle studentesse circa l'uso responsabile delle tecnologie e della Rete, elencando loro le regole della sicurezza online, **prima del primo accesso**.
L'accesso a Internet dovrà avvenire sempre e solo a scopo didattico, dietro autorizzazione e sotto lo stretto controllo dei docenti stessi, i quali provvederanno anche a suggerire **per lo studio a scuola e a casa siti web e risorse digitali utili, sicuri, idonei ed educativi**.
Nelle classi prime, in particolare, ci si procurerà di includere una discussione guidata sulla e-policy della scuola nel **protocollo di accoglienza** che concerne le attività dei primi giorni di scuola.
La e-policy della scuola verrà inoltre comunicata e discussa negli **organi collegiali (Consigli di Classe e interclasse, riunioni dipartimentali, Collegio Docenti e Consiglio d'Istituto**), nei quali sarà messa all'ordine del giorno a inizio di ogni anno e in caso di variazioni in itinere.
La scuola promuove **eventi e dibattiti formativi e informativi, anche con il coinvolgimento di esperti, e attività di *peer education* sulla sicurezza online**.
Essa mette, inoltre, in atto azioni volte a diffondere una cultura dell'inclusione, del rispetto delle differenze e a sviluppare le competenze emotive, in modo da favorire la corretta gestione del digitale come strumento relazionale.

1.5 - Gestione delle infrazioni alla Policy.

Le infrazioni alla e-safety policy da parte di studentesse e studenti possono configurarsi come infrazioni lievi, casi gravi e veri e propri reati.
Esse includono: ***l'uso di siti e strumenti non espressamente autorizzati dai docenti durante le lezioni o per visualizzare o scaricare materiali non consentiti; l'uso non autorizzato del cellulare durante l'orario scolastico; l'uso di social network in orario scolastico; l'invio di messaggi, foto e/o e-mail inappropriati; la violazione della privacy altrui; l'accesso a, il download e la diffusione di materiali offensivi, diffamatori, omofobici, razzisti, discriminatori e/o violenti; la produzione di riprese audio e/o video non autorizzate; la violazione dei diritti d'autore; l'invio di offese e insulti tramite messaggi di testo, e-mail o social network, l'esclusione da gruppi online (e tutti gli atti configurabili come cyberbullismo); il furto d'identità; il possesso di foto o video che riproducono situazioni violente, intime o offensive; il furto e l'uso illecito di credenziali; la frequentazione di siti pro-suicidio, pro-bulimia e/o pro-anoressia; il gioco d'azzardo online.***
Per quanto concerne, in particolare, l'uso dei cellulari, è fatto divieto assoluto agli studenti e alle studentesse di utilizzarli in ogni ambiente scolastico senza il permesso dei docenti e/o di tenerli accesi negli zaini. **L'utilizzo è consentito solo durante attività didattiche nelle modalità espressamente autorizzate dai docenti.** Per motivi di emergenza, gli alunni possono sempre utilizzare il telefono della scuola. È, inoltre, fatto divieto di utilizzare qualsiasi strumento fotografico o da ripresa o da riproduzione musicale, se non espressamente autorizzati dai docenti **(*Regolamento d'Istituto, art. 21*).**
Le infrazioni possono essere rilevate da tutto il personale scolastico nell'esercizio delle proprie funzioni, nonché da studenti e studentesse e dai loro genitori, che ne informeranno i docenti responsabili della sicurezza online.
Per la gestione si fa riferimento al ***Regolamento d'Istituto (art. 21)***, che prevede, in base alla gravità, le seguenti azioni: *ammonizioni verbali e/o scritte* sul registro elettronico e relativa comunicazione verbale e/o scritta alla famiglia; *censura formale* da parte del Consiglio di Classe/Interclasse e comunicazione scritta della stessa alla famiglia; *sanzioni disciplinari* di crescente entità (che possono arrivare fino a 15 giorni) per gravi offese alle persone, per aver diffuso immagini con dati personali altrui non autorizzate e per oltraggio alla religione di qualunque confessione e alla morale.

Gli interventi correttivi previsti saranno rapportati all'età e al livello di sviluppo degli studenti e delle studentesse e la loro finalità sarà sempre educativa (e mai punitiva), e cioè volta al ripristino di comportamenti corretti e allo sviluppo di una crescente consapevolezza delle regole sociali e delle competenze relazionali e affettive nel mondo digitale e non. Alle studentesse e agli studenti sarà offerta la possibilità di commutare le sanzioni in attività a favore della comunità scolastica (e, in particolare, attività di ricerca e approfondimento su regolamenti e/o norme violati e socializzazione della propria esperienza con i compagni/e a fini preventivi).
Qualora le infrazioni si configurino come reati veri e propri commessi all'interno della scuola in ambito digitale, lo si segnalerà tempestivamente al Dirigente stesso, che procederà agli **adempimenti di legge previsti**.
Le azioni da attuare, in ogni caso in cui si sospettino attività illegali, sono: la conservazione delle prove e il fare rapporto alle autorità competenti.
Tutto il personale scolastico, pena sanzioni disciplinari e, in casi più gravi, civili e penali, è tenuto a rispettare e promuovere il rispetto delle seguenti regole: non effettuare azioni illegali e/o che possano nuocere ai minori; evitare comportamenti digitali compromettenti; non utilizzare i sistemi di condivisione (messaggi, email) per inviare materiali inappropriati (come, ad esempio, molestie e messaggi d'odio e violenti); seguire il ***Regolamento d'uso del laboratorio informatico***; non utilizzare Internet all'interno della scuola per attività personali non legate allo svolgimento della professione; usare supporti esterni di memorizzazione dei dati considerandone l'adeguatezza e implementando corrette procedure di salvaguardia di qualsiasi file memorizzato; mettere in atto tutte le misure di sicurezza necessarie nell'utilizzo delle attrezzature e nella gestione protetta dei dati, in particolare di quelli personali; utilizzare lecitamente copyright e licenze software; rispettare tutte le condizioni d'uso di hardware e software.

1.6 -Monitoraggio dell'implementazione della Policy e suo aggiornamento.

Al termine di ciascun anno scolastico, l'animatore digitale e il docente referente per il cyberbullismo, con la collaborazione dei docenti funzioni strumentali dell'area 4 (Gestione risorse tecnologiche e informatiche) e con la supervisione del Dirigente Scolastico, effettuano attività di verifica dell'impatto e dell'efficacia della e-policy nella scuola.
Dette attività includono anzitutto **l'analisi degli eventuali casi problematici rilevati e della loro gestione**, **nonché delle segnalazioni e delle richieste da parte dei docenti, degli studenti e delle studentesse e dei loro genitori, anche in base alla introduzione di nuove tecnologie.**
Se i riscontri dovessero rivelarsi insufficienti, si predisporranno questionari da somministrare ai docenti, allo scopo di far insorgere eventuali problematiche e richieste non altrimenti palesatesi.
Sulla base di quanto analizzato, se constatata l'opportunità di modifiche e/o integrazioni, all'inizio dell'anno scolastico successivo, si provvederà all'aggiornamento della e-policy d'istituto.
L'adeguatezza del documento verrà monitorata in via straordinaria, nel corso dell'anno scolastico, ogni volta che si verifichino cambiamenti significativi delle tecnologie in uso nella scuola e/o vengano emanate nuove indicazioni dal Miur, dall'Unione Europea e dal *SIC Italy*.
Tutte le modifiche, supervisionate dal **Dirigente Scolastico**, saranno presentate al **Collegio Docenti** e ratificate dal **Consiglio d'Istituto**, per garantire che tutta la comunità scolastica condivida la e-policy d'istituto.

1.7 - Integrazione della Policy con Regolamenti esistenti.

Il documento di e-policy si integra con gli obiettivi e i contenuti del **PTOF**, con particolare riferimento al **piano digitale** della scuola ivi incluso, con il **RAV**, con il ***Regolamento d'Istituto,*** con il ***Patto***

Educativo di Corresponsabilità, con il ***Regolamento d'uso del laboratorio informatico*** e con il ***Regolamento d'uso dei cellulari a scuola.***
Pertanto, saranno previste attività volte a rendere sempre coerenti tutte le politiche e la documentazione della scuola, in ragione delle modifiche eventualmente apportate alla e-policy.

2. Formazione e curricolo

2.1 - Curricolo sulle competenze digitali per gli studenti.

Le **Indicazioni Nazionali del 2012**, richiamando la **Raccomandazione Europea del 2006 per il Lifelong Learning**, pongono le competenze digitali tra le competenze chiave da certificare al termine del primo ciclo. Per questo, il curricolo verticale del nostro istituto promuove lo sviluppo delle competenze d'uso delle tecnologie dell'informazione e della comunicazione, **cui concorrono non solo abilità più strettamente tecniche, ma anche critiche, di analisi, controllo e verifica di dati e informazioni (per valutarne l'attendibilità e l'appropriatezza) e di interazione (per una partecipazione corretta, consapevole e attiva alla società digitale)**. Ciò comporta la progressiva educazione alla sicurezza online che prevede, dunque, comportamenti appropriati e il riconoscimento, l'evitamento e la capacità di segnalazione corretta di fenomeni quali il cyberbullismo o il download e l'upload di file e foto senza le necessarie autorizzazioni.
Pur implicando il piano digitale della nostra scuola un ***aggiornamento del curricolo di Tecnologia*** (volto precipuamente allo sviluppo delle competenze digitali per gli studenti e le studentesse), le competenze digitali sono nel contempo perseguite anche **trasversalmente a tutte le discipline** del curricolo, in quanto tutte concorrono alla loro costruzione.
A questo scopo, i docenti hanno la possibilità di implementare attività didattiche sulla sicurezza online mediante l'utilizzo di appositi **kit messi a disposizione della scuola dal progetto Generazioni Connesse (www.generazioniconnesse.it)**.
Inoltre, l'istituto ha provveduto ad assegnare ***a docenti diversi l'insegnamento delle discipline di Matematica e Scienze*** nella scuola primaria e secondaria di secondo grado, ponendo tra i risultati attesi da questa azione proprio lo sviluppo delle abilità del coding e del pensiero computazionale. In questa direzione vanno anche le adesioni della scuola a diversi progetti che hanno tra i loro obiettivi la certificazione delle competenze informatiche degli alunni attraverso diversi percorsi Eipass: Basic, 7 moduli user e Web; "***Programmare il futuro***", per l'accessibilità al coding; "***Generazioni connesse***", per la promozione di un uso sicuro e consapevole della Rete negli alunni/e delle classi quarte e quinte della scuola primaria e negli studenti e studentesse della scuola secondaria di primo grado. Infine, concorre all'educazione civica digitale come dimensione trasversale ai diversi saperi anche l'adesione al progetto in rete "***Educare alla legalità e alla cittadinanza attiva***".

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

Il corpo docente del nostro istituto possiede in genere buone competenze digitali di base: utilizza il registro elettronico, corrisponde per e-mail (avendo la nostra scuola, in ottemperanza alla Legge n. 135/2012, dematerializzato le comunicazioni istituzionali), usa in genere la LIM e il computer nella didattica; mentre alcuni di loro possiedono conoscenze avanzate (in particolare, le funzioni strumentali dell'area 4).

Ma, poiché il piano digitale della scuola si pone l'obiettivo di rendere l'offerta formativa sempre più coerente con i cambiamenti della società e rispondente alle esigenze di apprendimento e agli stili cognitivi degli studenti e delle studentesse, risulta indispensabile promuovere sempre più la formazione continua dei docenti sulle TIC, volta proprio all'innovazione della didattica. Per questo, un nutrito gruppo di docenti ha partecipato a corsi di formazione anche nell'ambito di piani nazionali o organizzati dalla rete di scuole, finalizzati all'innovazione delle metodologie e delle strategie didattiche. Tra questi, il progetto "***Pekit One Project: Digital Lesson***" (Polo Qualità di Napoli) e il progetto "***Dalla lezione all'interazione***" (Microsoft, USR Campania e Polo Qualità di Napoli).
Inoltre, l'animatore digitale ha realizzato, nel corso dell'anno scolastico 2015-16, un corso di alfabetizzazione digitale per gli insegnanti della scuola dell'infanzia e primaria e, nell'anno scolastico 2017-18, ha somministrato **un questionario finalizzato a rilevare i bisogni digitali di tutti docenti della scuola e a mettere conseguentemente a loro disposizione corsi di formazione e/o aggiornamento per piccoli gruppi** (per consentire l'operatività e l'applicabilità immediata di quanto appreso) sull'uso del digitale nella didattica e su piattaforme e app per l'apprendimento (a partire da marzo 2018 con l'animatore digitale stesso come formatore). Sono, infine, periodicamente divulgati, sempre a cura dell'animatore digitale, corsi di aggiornamento online (anche gratuiti) per docenti.

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

Nell'anno scolastico 2017-18 un gruppo di docenti afferenti ai diversi plessi e gradi del nostro istituto ha partecipato a un corso di formazione sulla sicurezza online tenuto da un esperto di Telefono Azzurro. Un secondo corso, tenuto dagli esperti dell'Associazione Nirvana e da rappresentanti delle Forze dell'Ordine, è stato destinato a tutti i docenti della scuola.
L'adesione della scuola al progetto Generazioni Connesse consente, inoltre, a tutti i docenti della scuola anche di attingere a corsi di formazione online (dedicati a diverse aree tematiche, come *l'educazione ai e con i media, l'uso delle tecnologie a scuola e l'inclusione e la partecipazione*), nonché a vademecum, materiali e risorse sulla sicurezza online precipuamente rivolti alla formazione dei docenti.
Video, guide in pdf, link a siti specializzati (come appunto a quello di "Generazioni Connesse", che, a sua volta, rinvia a siti di partner, quali "**Telefono Azzurro**" e "**Save the children**") sono reperibili sul sito della scuola, nell'apposita sezione "Osservatorio cyberbullismo".

2.4 - Sensibilizzazione delle famiglie.

I momenti di confronto informali dei docenti e della dirigenza con le famiglie, finalizzati a dare continuità alle regole e alla linea adottata dalla scuola sulla sicurezza online, sono quasi quotidiani, anche perché le modalità d'uso dello smartphone (a scuola e fuori) sono argomento di continuo dibattito. La collaborazione con le famiglie nel perseguire l'adeguatezza e la sicurezza nell'uso delle TIC viene costantemente incoraggiata anche in occasione degli **incontri scuola-famiglia, collegiali, assembleari e individuali.**
Inoltre, sono stati predisposti, per le famiglie, un seminario con un esperto di Telefono Azzurro e un incontro con gli esperti dell'Associazione Nirvana, finalizzati proprio a sensibilizzare i genitori perché vigilino e stabiliscano regole d'uso, nonché dialoghino con i ragazzi e le ragazze, per far emergere eventuali problematiche.
L'invito a rivolgersi agli esperti di Telefono Azzurro, in caso di dubbi e incertezze, e a consultare il sito di Generazioni Connesse (nell'apposita sezione dedicata ai genitori), oltre che durante il seminario, è anche ripetuto sul nostro sito istituzionale.

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

3.1 – Gestione accessi.

Il nostro istituto è costituito da cinque plessi. Nei due edifici della scuola secondaria di I grado è presente e utilizzata la connessione Wi-fi, realizzata grazie alla partecipazione al progetto per la realizzazione/ampliamento rete LAN/WLAN; sono presenti PC notebook portatili collegabili alle LIM (disponibili nella maggioranza delle aule) e nei laboratori informatico e linguistico (dotati di diverse postazioni PC e utilizzati entrambi per attività curricolari ed extracurricolari); ci sono anche auditorium attrezzati per videoproiezioni e utilizzati per seminari, corsi di formazione per i docenti e attività scolastiche varie. Interventi periodici di manutenzione sono previsti grazie a una figura con incarico specifico.
Nei plessi della scuola primaria è presente un'aula LIM, ma non vi sono laboratori informatici a più postazioni.
I computer dei laboratori sono dotati di firewall e software antivirus per proteggere le connessioni in entrata e in uscita.
Il personale amministrativo possiede password personali per l'accesso ai dati personali di studentesse e studenti e di tutto il personale dell'istituto. La modalità di backup è su computer-server, il cui accesso è riservato solo agli assistenti amministrativi e alla dirigenza.
L'accesso degli utenti (docenti e personale scolastico) alla rete Wi-fi è consentito attraverso il riconoscimento delle credenziali: la password non è comune ed è legata al proprio indirizzo istituzionale fornito dal Miur.
I docenti possono, quindi, accedere a Internet dai propri dispositivi o da quelli in dotazione della scuola, mediante un meccanismo di identificazione e autorizzazione che consente l'accesso solo da un dispositivo per volta, e sono quindi responsabili delle azioni svolte attraverso il medesimo.
La password di accesso alla rete wireless deve essere custodita con cura e non può essere divulgata a chi non ha titolo per utilizzarla (studenti e studentesse, genitori, operatori esterni).
L'uso improprio della rete è contestato al titolare delle credenziali. Questi verificherà, inoltre, sempre il corretto spegnimento del device utilizzato.
L'impiego di notebook e postazioni fisse è annotato mediante firma su appositi registri, sui quali vengono appuntate anche attività, orari ed eventuali classi destinatarie, nonché le anomalie, se verificatesi.
L'accesso ai portali istituzionali (come Istanze online, NOIPA, SIDI, INDIRE) avviene mediante l'uso di credenziali personali; mentre l'accesso a portali relativi a progetti a cui la scuola aderisce (come Generazioni Connesse), avviene mediante la condivisione di password uniche tra i referenti dei progetti stessi.
Gli studenti e le studentesse possono accedere a Internet mediante connessione alla rete della scuola dalle postazioni nei laboratori informatici e linguistici. Ogni classe è tenuta a definire postazioni fisse, per la rintracciabilità in caso di problematiche di carattere tecnico e/o legate alla navigazione poco sicura.
La scuola promuove anche la metodologia BYOD, mediante la quale, per attività didattiche per le quali i docenti ne ravvisino l'opportunità, e sotto la loro stretta vigilanza, gli alunni possono utilizzare i propri dispositivi (tablet e smartphone).

3.2- E-mail.

Tutte le comunicazioni della scuola al personale scolastico avvengono attraverso gli indirizzi e-mail istituzionali (naic8en005@istruzione.it; naic8en005pec.istruzione.it; info@icninocortese.gov.it) e dell'animatore digitale.

Le comunicazioni scuola-famiglia avvengono invece soprattutto attraverso il registro elettronico, dove i docenti, il Dirigente Scolastico e il personale di segreteria annotano avvisi, assenze, ritardi, voti.
La scuola non rende pubblici indirizzi di posta elettronica degli alunni, delle famiglie e del personale tutto.
Vengono adottate tecnologie apposite per la protezione dell'istituto e dei suoi utenti, attraverso sistemi antivirus sui singoli PC.
Ma, se il personale scolastico o gli alunni dovessero ricevere e-mail inopportune o non lecite, dovranno essere tempestivamente informati il Dirigente Scolastico e l'animatore digitale.

3.3- Sito web della scuola

L'istituto dispone di uno spazio web e di un dominio (www.icninocortese.gov.it) la cui gestione è a cura dell'animatore digitale, previa autorizzazione delle pubblicazioni da parte del Dirigente Scolastico.
Quanto pubblicato viene valutato in base ai criteri di pertinenza e di appropriatezza e ha finalità educative e didattiche.
Il sito presenta due aree: una pubblica e l'altra riservata. In quella pubblica, accessibile a tutti, vengono caricati comunicazioni ufficiali e avvisi inerenti il funzionamento e le attività dell'istituto, foto e video riguardanti momenti significativi della vita scolastica, materiali didattici per le studentesse e gli studenti e strumenti per i genitori, la documentazione riguardante attività curricolari ed extracurricolari, la modulistica, le iniziative e le scadenze della scuola e ministeriali. Nell'area riservata, a cui si accede previa autenticazione, vengono pubblicate comunicazioni, circolari, avvisi e strumenti e materiali rivolti al personale scolastico. In questo caso, il sito registra i dati forniti dagli utenti per il riconoscimento di username e password, necessari per fornire i servizi richiesti.
Il sito rimanda poi a piattaforme correlate (come Iscrizioni online), alle quali è possibile accedere mediante autenticazione.

3.4 - Social network.

L'istituto dispone di una pagina facebook con il proprio profilo e di un canale You tube, sui quali pubblica soprattutto video e immagini che documentano momenti significativi delle attività e che divulgano le iniziative scolastiche, come i progetti, le attività nei vari laboratori, le manifestazioni musicali e teatrali, gli incontri con autori e personalità.
I criteri di selezione delle pubblicazioni sono il rispetto della dignità personale e il decoro dell'istituto.
La scuola promuove, infatti, un uso appropriato dei social network: quindi, il personale e gli studenti e le studentesse sono tenuti a realizzare, prelevare e diffondere immagini, video e registrazioni audio, solo se autorizzati e mai se contenenti riferimenti inopportuni e offensivi a studenti, a studentesse, ai docenti, a tutto il personale scolastico e all'istituto stesso.
La scuola promuove l'utilizzo delle piattaforme di apprendimento che consentono di gestire la classe come gruppo virtuale: in particolare, vengono utilizzati **Edmodo, Fidenia e Google Classroom**. Questi consentono una nuova e più inclusiva interazione tra docenti e studenti e studentesse, permettendo di produrre e fornire materiali e di progettare le attività diversificando modalità e ritmi.
Mentre ogni docente può usufruire delle piattaforme Edmodo e Fidenia in autonomia, per Google Classroom è necessario che l'istituto sia iscritto all'ambiente virtuale G Suite for Education, perché ogni utente (docente e studenti e studentesse) possa avere uno spazio virtuale ed un indirizzo e-mail con "dominio" della scuola (www.icninocortese.gov.it). Inoltre, mentre per l'iscrizione a Edmodo e Fidenia basta creare un account (nome utente e password), con e-mail facoltativa, Google Classroom richiede obbligatoriamente l'e-mail.

I minori di 13 anni possono accedere al servizio con delle limitazioni e, per poter iscrivere gli alunni/e, è sempre necessario acquisire dai genitori degli stessi una **liberatoria**, il cui modello è prodotto dalla scuola.
Si auspica che in futuro, dopo una prima fase di sperimentazione, l'istituto possa arrivare a condividere un'unica piattaforma, anche al fine di favorire lo scambio di esperienze tra i docenti.

3.5 - Protezione dei dati personali.

In base all'art.1 D.Lgs.196/2003 della legge sulla privacy, la nostra scuola garantisce il "*diritto alla riservatezza delle informazioni personali e della propria vita privata*"; pertanto, **i dati personali del personale scolastico e degli studenti e delle studentesse e delle loro famiglie non vengono divulgati o conferiti a terzi senza il consenso dell'interessato o di chi esercita la tutela e sono trattati nel rispetto delle regole e dei principi stabiliti dalla legge** come attuativi del diritto alla privacy *(**Codice in materia di protezione dei dati personali** - Decreto legislativo 30 giugno 2003, n.196 e successive modifiche e integrazioni).*
Per **dato personale** si intende "*qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale"* (art. 4 D.lgs 196/2003). Essi includono: i **dati sensibili** (*"i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale");* i **dati identificativi** ("*i dati personali che permettono l'identificazione diretta dell'interessato*"); i **dati giudiziari** (" *i dati personali idonei a rivelare provvedimenti", "in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti o la qualità di imputato o di indagato").*
Il Titolare del trattamento dei dati è l'Istituto I.C. Nino Cortese, nella persona del suo legale rappresentante pro tempore. Il Responsabile per la gestione e il controllo dei dati è il DSGA. Nei limiti dello svolgimento delle proprie funzioni, il personale scolastico (docente e amministrativo) è incaricato del trattamento dei dati in possesso della scuola ed è tenuto ad attenersi a criteri di correttezza, trasparenza e liceità e a non comunicarli a terzi, se non per usi di legge.
Il consenso dell'interessato o di chi ne esercita la tutela non è richiesto se si esercita per il perseguimento di specifiche finalità istituzionali ovvero quelle espressamente previste dalla normativa di settore. Viene richiesta autorizzazione al trattamento dei dati (e fornita relativa comunicazione con informativa specifica) ai genitori dei bambini/e che vengono iscritti alla scuola dell'Infanzia.
Viene, inoltre, richiesta **liberatoria** in cui chi ne esercita la tutela autorizza la scuola a riprendere e/o a far riprendere in video e/o a fotografare gli alunni/e, in occasione di viaggi, visite d'istruzione e partecipazione a eventi connessi all'attività didattica (da soli, con i compagni, con insegnanti e operatori scolastici), ai fini di formazione, ricerca e documentazione dell'attività didattica (come cartelloni all'interno della scuola o in occasione di esposizioni esterne); divulgazione della ricerca didattica e delle esperienze effettuate sotto forma di documento in ambiti di studio (ad es. su DVD, sul sito web della scuola o su altri siti autorizzati); stampe e giornalini scolastici; partecipazione a iniziative di sensibilizzazione alle problematiche sociali.
Tutti i membri della nostra comunità scolastica, quindi, non diffondono e comunicano i dati di altre persone (ad esempio, pubblicandoli sul web) senza averle prima informate adeguatamente e aver da loro ottenuto esplicito consenso.
I genitori potranno riprendere immagini e video di manifestazioni scolastiche, gite, recite, ma solo per utilizzo personale e se destinate all'ambito familiare. Detti immagini e video non verranno quindi mai pubblicati su Internet senza il consenso esplicito degli interessati.
Si consente agli studenti con DSA, ove previsto dal PDP, la registrazione delle lezioni, per utilizzo strettamente personale.

4. Strumentazione personale

4.1 - Per gli studenti: gestione degli strumenti personali.

Gli studenti e le studentesse dovranno custodire i loro cellulari e tablet spenti all'interno degli zaini e potranno utilizzarli solo dietro espressa autorizzazione dei docenti, in specifici momenti in cui è previsto dalle attività di apprendimento progettate. **I cellulari possono essere di nuovo accesi solo fuori dei cancelli esterni**. È fatto **assoluto divieto di portare i cellulari in alcun ambiente scolastico: nei bagni, nei laboratori, in palestra e negli ambienti comuni.**
Durante l'utilizzo a scopo didattico, gli studenti e le studentesse non potranno accedere a chiamate, a messaggi e a social network, o comunque usare il cellulare per comunicazioni personali.
Foto e riprese audio e/o video dovranno essere effettuate solo se previste dall'attività e se espressamente autorizzate dai docenti. Si evidenzia, in particolare, la gravità di eventuali riprese audio/video o fotografie effettuate e successivamente diffuse con l'intento di ridicolizzare compagni/e o docenti o addirittura di intraprendere atti di cyberbullismo, che possono configurare, nei casi più gravi, gli estremi di veri e propri reati.
Gli studenti con DSA e altri bisogni educativi speciali, se previsto dal Consiglio di Classe all'interno del PDP, potranno utilizzare i loro device nelle modalità ivi approvate. Inoltre, se ratificato dal Consiglio di Classe, detto utilizzo potrà essere condiviso con gli altri alunni/e a fini inclusivi.
Durante le uscite didattiche e i viaggi di istruzione, l'uso dei cellulari è consentito al di fuori dei momenti dedicati a visite guidate e altre attività strettamente legate all'aspetto didattico dell'uscita.
La violazione di tali disposizioni configura un'infrazione disciplinare rispetto alla quale la scuola è tenuta ad applicare apposite sanzioni, come da ***Regolamento d'Istituto (art.21)***.

4.2 - Per i docenti e per il personale della scuola: gestione degli strumenti personali.

Non è consentito ai docenti l'utilizzo di cellulari durante le lezioni, se non a scopi didattici e a integrazione dei dispositivi in dotazione nella scuola.
La responsabilità della custodia e della corretta gestione degli strumenti personali (cellulari, tablet, ecc.) è esclusivamente a cura e di responsabilità del proprietario.
L'utilizzo del cellulare a scopi personali all'interno della scuola è consentito ai docenti e al personale ATA solo per comunicazioni urgenti, purché ciò non interferisca con il corretto svolgimento del servizio.

5. Prevenzione, rilevazione e gestione dei casi

5.1– Prevenzione dei rischi: le azioni

L'educazione rappresenta il principale strumento di prevenzione: per questo, la scuola ha programmato numerose attività volte a sviluppare le capacità di riconoscere e gestire i rischi e i disagi online e a prevenire le problematiche derivanti da un uso poco sicuro e consapevole delle nuove tecnologie e della Rete, e, in particolare, il bullismo e il cyberbullismo, in ottemperanza **all'art. 1 comma 7 della Legge 107/2015 (che individua la prevenzione e il contrasto del cyberbullismo tra gli obiettivi formativi prioritari) e delle Linee Guida della Legge 71/2017**. Questa reca le "*Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo (*e, cioè *"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti online aventi ad oggetto anche uno o più componenti della famiglia del minore 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")*. Ai sensi dell'art. 4, co. 3, l'Istituto ha individuato un ***docente referente con il compito di coordinare le attività di prevenzione e di contrasto del cyberbullismo.***

Le attività volte a sviluppare il senso di responsabilità e il rispetto dei regolamenti nel mondo fisico e in quello digitale sono trasversali alle discipline e rafforzate da azioni finalizzate all'educazione all'affettività, al riconoscimento e alla risoluzione dei conflitti, nonché da iniziative volte alla promozione della cultura della diversità come ricchezza e al riconoscimento che ogni persona è degna di rispetto.

Attraverso l'insegnamento-apprendimento dell'educazione civica digitale, le nostre studentesse e i nostri studenti devono essere resi consapevoli e corretti nell'uso della Rete, per non arrecare danni a se stessi e ad altri, e, per questo, viene loro insegnato a: ***evitare di diffondere in rete informazioni personali (come l'indirizzo di casa o la scuola che si frequenta); proteggere i propri dati sensibili, creando password complesse e non rivelandole a terzi, nonché controllando le impostazioni della privacy, se utilizzano social network; chiedere agli amici il permesso esplicito di postare immagini in cui compaiono e far sì che essi facciano altrettanto; limitare l'abitudine di postare e condividere in maniera eccessiva; usare videogiochi educativi e sicuri; informarsi in Rete con senso critico.***

Per quanto concerne, in particolare, il cyberbullismo, alle studentesse e agli studenti viene poi insegnato a: ***non inviare messaggi violenti diretti ad accendere battaglie verbali (flaming) e/o messaggi offensivi, finalizzati a ferire (harassment); non danneggiare la reputazione degli altri (denigrazione); non spacciarsi per qualcun altro (impersonation); non rivelare informazioni private altrui (exposure e/o trickery); non escludere una persona da un gruppo online; non molestare e perseguitare online (cyberstalking).***

Perché le studentesse e gli studenti acquisiscano queste competenze, è prima necessario che siano formati e/o informati i docenti e le famiglie. Quindi è caldamente richiesta la loro **partecipazione alle iniziative formative e informative della scuola e la piena collaborazione nell'educazione e nella vigilanza**.

Corsi di formazione e seminari su queste tematiche sono stati tenuti da un esperto di Telefono Azzurro, che, nel mese di novembre 2017, ha: aggiornato un **gruppo di docenti rappresentativo dei vari plessi e segmenti** della scuola; avuto un incontro informativo con i **genitori,** seguito da un dibattito sulle regole da condividere circa l'uso dei cellulari; tenuto corsi di formazione per **gli alunni delle classi terze della scuola secondaria di primo grado**.

Mediante lettera circolare (*Prot.617/B10*), è stato inoltre richiesto a tutti i docenti della scuola di **visitare il sito del progetto Generazioni Connesse (www.generazioniconnesse.it)**, affinché, attraverso l'aggiornamento e l'informazione, possano attingere materiali e spunti per la didattica in classe e possano sviluppare lo scambio di consigli e suggerimenti e il confronto di esperienze tra tutti gli insegnanti della scuola, in particolare sugli aspetti relazionali delle nuove tecnologie. Anche i genitori sono stati invitati a connettersi al sito del progetto, durante gli incontri e mediante ripetuti annunci sul sito della scuola.

Nel mese di gennaio 2018, l'animatore digitale e il referente per il cyberbullismo hanno poi formato un gruppo di dieci studentesse e studenti delle classi terze e seconde della secondaria di primo grado (scelti in base alle capacità relazionali e alle competenze sul tema e tra quelli che avevano partecipato al corso Eipass), perché tenessero una lezione intitolata "Chi è il cyberbullo?" **alle studentesse e agli studenti delle classi prime e seconde.** Il focus della lezione era sul cyberbullismo e sui rischi derivanti da un uso non responsabile del web (evidenziando gli strumenti per la prevenzione, ma anche gli aspetti positivi della Rete come strumento di conoscenza e relazione!). Al termine dell'esperienza di **peer education**, ciascuna classe ha realizzato un proprio logo word art contro il bullismo e il cyberbullismo.
Attività didattiche in classe sono state programmate per il mese di marzo 2018 anche nelle **classi quarta e quinta della scuola primaria**, mediante l'utilizzo degli appositi kit didattici proposti dal progetto "Generazioni Connesse".
Nell'ambito del progetto "Ciak si gira", come già durante lo scorso anno scolastico, è prevista invece la realizzazione di cortometraggi con le studentesse e gli studenti come attori, volti a diffondere messaggi educativi sull'uso corretto della Rete, sul bullismo e sul cyberbullismo.
Sono stati poi organizzati, nei mesi di febbraio e marzo 2018, per tutti i docenti, per tutti gli studenti e le studentesse della secondaria di primo grado e della scuola primaria, nonché per i loro genitori, momenti formativi con gli esperti dell'Associazione Nirvana, con la collaborazione di rappresentanti delle Forze dell'Ordine. Essi si occupano di **sicurezza online (e, in particolare, di cyberstalking) e parità di genere**.
Sono, inoltre, previsti, come consuetudine ad ogni anno scolastico, incontri formativi di educazione alla legalità rivolti agli studenti e alle studentesse della nostra scuola, organizzati dai **Carabinieri della Caserma Stazione di Arpino,** volti alla prevenzione del disagio giovanile, prestando particolare attenzione alle problematiche legate a un utilizzo non sicuro di Internet.
Nel mese di marzo si è svolta anche una visita guidata presso la Prefettura di Napoli, nell'ambito del Progetto **"Istituzioni e media..incontro ai ragazzi**", alla quale ha partecipato un gruppo di circa 25 studenti e studentesse delle classi terze della scuola secondaria di primo grado.
Nella programmazione del **Progetto Cineforum** per il prossimo anno scolastico, la referente dell'area uscite didattiche ha poi inserito tra le tematiche da trattare anche il bullismo e il cyberbullismo. Prima e dopo la visione di un film sul tema, i docenti di Lettere organizzeranno attività di approfondimento specifiche in classe.
La scuola aderisce infine alle campagne contro il bullismo e il cyberbullismo e le diffonde sul proprio sito web. Lo scorso anno scolastico, in occasione della giornata per la prevenzione del bullismo "Un nodo blu" è stato organizzato un flash mob; mentre quest'anno è stato indetto il concorso interno per realizzare e scegliere il logo per il nostro "Osservatorio cyberbullismo".

5.2– Rilevazione: quali strumenti; cosa e come segnalare.

La scuola intende creare una memoria condivisa di ciò che di problematico riguardo all'uso della rete accade. A questo scopo, viene adottato il *"diario di bordo" proposto dal sito di "Generazioni Connesse",* in allegato al presente documento.
Il primo strumento per la rilevazione di problematiche è da considerarsi l'**osservazione sistematica,** per valutare eventuali segnali di disagio e difficoltà da approfondire con gli altri docenti del Consigli di Classe e con la famiglia.
Gli esperti suggeriscono indicatori che possono aiutare a identificare casi di bullismo e cyberbullismo (e altri disagi legati all'uso improprio della Rete), ma che, tuttavia, non li denotano in modo assoluto, soprattutto se considerati isolatamente.
Tra i possibili indicatori di fenomeni di vittimizzazione da bullismo e cyberbullismo ci sono: la difficoltà ad andare a scuola e le assenze frequenti senza motivi concreti; i segni di percosse e violenza fisica; il danneggiamento e/ la dispersione di oggetti e beni personali; le paure apparentemente ingiustificate; lo stato di allerta; l'ansia; l'insicurezza; la bassa autostima; la chiusura e l'isolamento sociale; l'esclusione da gruppi di messaggistica istantanea; i disturbi del sonno; il rendimento scolastico

discontinuo; la difficoltà a gestire le emozioni; l'eccessiva reattività; l'iperattività; la difficoltà di attenzione; la ricerca della compagnia degli adulti (piuttosto che di quella dei pari).
Indicatori di comportamenti da bullo o cyberbullo possono includere: i comportamenti prevaricatori; un'apparente alta autostima; la scarsa propensione a collaborare con gli altri; gli atteggiamenti di dominanza durante i lavori di gruppo; la scarsa empatia; lo scarso rendimento scolastico.
Perché gli eventi di bullismo e cyberbullismo vengano rivelati dalle vittime o dai loro compagni ai docenti, è raccomandato da parte di questi ultimi un atteggiamento accogliente, affettivo ed empatico, che faciliti le confidenze e le segnalazioni.
Altro strumento per la rilevazione è lo **"Sportello d'ascolto"**, gestito da quattro insegnanti scelti dal Collegio Docenti proprio perché hanno dimostrato di possedere le caratteristiche appena menzionate. Essi tengono un diario di bordo specifico.
Sono state inoltre predisposte **cassette postali** dove, anche in forma anonima, le studentesse e gli studenti possono segnalare al Dirigente Scolastico disagi e problematiche (ma anche suggerimenti) di ogni tipo.
Un ulteriore strumento per la rilevazione di situazioni problematiche è il **questionario somministrato in forma anonima.** Esso, oltre che di far emergere eventuali casi di bullismo e cyberbullismo, si propone di delineare lo stato generale delle relazioni (incluse quelle con i docenti e con la dirigenza) nei luoghi fisici e digitali frequentati dalle nostre studentesse e dai nostri studenti, allo scopo di migliorarle.
Al termine dell'attività "Ciak si gira: facciamo rumore", in collaborazione dell'Associazione Nirvana, è stato anche previsto, su suggerimento degli stessi esperti dell'Associazione, di far elaborare alle studentesse e agli studenti un saggio in cui venissero esposte le riflessioni e le emozioni suscitate dal percorso formativo, ai fini di rilevare eventuali problematiche e disagi.
Nel caso dovessero essere rilevati, attraverso gli strumenti delineati e/o le attività laboratoriali in classe proposte sul sito Generazioni Connesse, saranno segnalati, in particolare, i seguenti abusi digitali: **l'uso di siti e strumenti non espressamente autorizzati dai docenti durante le lezioni o per visualizzare o scaricare materiali non consentiti; l'uso non autorizzato del cellulare durante l'orario scolastico; l'uso di social network in orario scolastico; l'invio di messaggi, foto e/o e-mail inappropriati; la violazione della privacy altrui; l'accesso a, il download e la diffusione di materiali offensivi, diffamatori, omofobici, razzisti, discriminatori e/o violenti; la produzione di riprese audio e/o video non autorizzate; la violazione dei diritti d'autore; l'invio di offese e insulti tramite messaggi di testo, e-mail o social network, l'esclusione da gruppi online e tutti gli atti configurabili come cyberbullismo; il furto d'identità; il possesso di foto o video che riproducono situazioni violente, intime o offensive; il furto e l'uso illecito di credenziali; la frequentazione di siti pro-suicidio, pro-bulimia e/o pro-anoressia; il gioco d'azzardo online.**
La segnalazione, in base alla gravità del caso, viene effettuata tramite **relazione verbale o scritta al Dirigente Scolastico e comunicazione verbale o scritta alla famiglia (che la vista per presa visione), avendo sempre cura di annotare quanto accaduto anche sul registro elettronico.**
Il docente, inoltre, compila l'apposito modello interno di segnalazione fornito dal Progetto Generazioni Connesse e allegato al presente documento; mentre il referente per il cyberbullismo registra l'evento sul diario di bordo, se la situazione rientra in questa problematica.
Il Dirigente Scolastico segnala sospetti illeciti alla Polizia Postale e delle Comunicazioni all'indirizzo www.commissariatodips.it. Il 114 è il numero di emergenza.

5.3 - Gestione dei casi: definizione delle azioni.

Il docente deve prima di tutto **rifuggire sia dal minimizzare sia dall'esagerare** i casi sospettati o rilevati**.** Poi è opportuno che **definisca il tipo di comportamento disfunzionale in cui si è imbattuto e che proceda secondo le indicazioni operative ad esso relative.** L'intervento, seppur tempestivo, deve essere sempre condiviso e deve tener conto dell'unicità degli alunni/e coinvolti/e nella situazione di difficoltà: il tipo di famiglia da cui l'alunno/a proviene (se è presente e se ha le risorse per affrontare la problematica oppure no); se l'alunno/a ha una rete di amici che possano supportarlo/a; il clima in classe; il contesto sociale; se l'alunno/a necessita del supporto dei servizi e istituzioni extra-scolastici. **Ciò che deve guidare il docente è sempre il superiore interesse del minore.**

Per una valutazione obiettiva dei casi, oltre al contesto, è necessario analizzare **le modalità in cui avvengono i presunti abusi (se in orario scolastico e/o extrascolastico; se alla presenza di un "pubblico"; se tra soli minori; se in modo cronico e intenzionale) e l'età dei protagonisti (si parla, ad esempio, di *cyberbullismo* solo se le persone coinvolte sono tutte minorenni).**

Se si ritiene di aver rilevato un errore o un abuso, anche non intenzionale, commesso da una studentessa o da uno studente utilizzando la Rete in maniera inidonea (o addirittura illecita), **è sempre necessario intervenire, fermando tempestivamente l'errore o l'abuso: i cellulari devono essere spenti immediatamente, senza cancellare le prove, che vanno conservate dalla vittima stessa** (il docente non deve invece effettuare download, produrre copie o condividere link).
Si possono prefigurare: **le infrazioni lievi** (come il mancato spegnimento intenzionale e/o l'utilizzo del cellulare senza l'autorizzazione del docente oppure non per l'attività didattica prevista), per cui, messo a parte il coordinatore di classe, lo si comunica (per lo più verbalmente) alla famiglia e lo si annota sul registro online; **i casi gravi** (come la produzione di immagini, audio e/o video non autorizzata, i casi di bullismo e cyberbullismo, la consultazione di siti e chat pro-suicidio, pro-anoressia, pro-bulimia, pro-autolesionismo, la dipendenza da Internet e dai videogiochi), per i quali, dopo aver compilato la scheda di segnalazione (se ci sono vittime e cyberbulli) e messo a parte il docente coordinatore (e, nei casi di cyberbullismo, il docente referente), è opportuno prendere in considerazione se convocare un Consiglio di Classe straordinario (alla presenza del Dirigente) per valutare le azioni da intraprendere, ivi incluse **le sanzioni disciplinari (il cui carattere sarà sempre educativo e mai punitivo, nonché, ove possibile, di utilità per la comunità),** redigere relativo verbale e produrre comunicazione scritta ai genitori (a cura del Dirigente) da far vidimare per presa visione e, se opportuno, contattare i servizi socio-sanitari**;** e, infine**,** i casi che includono **gli estremi del reato**, come furto di identità, cyberbullismo (nei casi sotto esplicitati), commercio on-line (nel caso di clonazione di carta di credito), pedopornografia on-line, grooming (adescamento on-line), gioco d'azzardo on-line, sexting, nei quali, acquisita la segnalazione, il Dirigente contatta le Forze dell'Ordine, perché possano approfondire la situazione da un punto di vista investigativo e attivare tutte le misure necessarie.
In tutti i casi in cui si rilevino problematiche e disagi per i minori, a seconda della necessità, la famiglia si potrà rivolgere a strutture pubbliche che offrono una consultazione generica (come lo studio del pediatra o del medico di base) o specifica (Consultorio Familiare, servizio di Neuropsichiatria Infantile) o a strutture specializzate (ad esempio, centri ospedalieri o servizi specializzati nelle dipendenze). Sono in corso lunghe e proficue collaborazioni in questo senso tra la scuola e i servizi neuropsichiatrici dell**'ASL di Casoria**.

La tempestività è particolarmente importante nei casi di **bullismo** e/o **cyberbullismo** (forme di prevaricazione e di oppressione reiterate nel tempo, perpetuate da una persona o da un gruppo nei confronti dei più deboli, offline e/o online) o di **sexting** (invio di messaggi con frasi e/o immagini intime), poiché in questi casi il pericolo è che immagini, commenti o notizie imbarazzanti si diffondano rapidamente, visto che i più giovani condividono o postano foto e informazioni personali nei social con facilità e la diffusione del materiale è incontrollabile (e non se ne possono prevedere i limiti!).
Per cyberbullismo, in particolare, s'intende ***"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti online aventi ad oggetto anche uno o più componenti della famiglia del minore 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 messa in ridicolo***" (**art. 1, comma 2, Legge n. 71/2017**).
A questo riguardo, nel momento in cui si contattano i genitori (a cura del Dirigente Scolastico), deve essere loro ricordato che, indicando tutti i riferimenti, possono richiedere **l'oscuramento** (mediante inoltro dell'apposita **istanza** reperibile sul sito di Generazioni Connesse e allegata a questo documento), **la rimozione di contenuti che possono ledere la dignità della persona o il blocco di dati e materiali riguardanti il minore, come garantito dalla Legge 71/2017.** La richiesta può essere fatta dal singolo utente e, qualora il gestore non la soddisfi, si può inoltrare analoga richiesta al Garante per la protezione dei dati personali.

In tutti i casi in cui immagini e/o video (anche prodotti autonomamente da persone minorenni) sfuggano al loro controllo e vengano diffuse senza il loro consenso, è sempre possibile, inoltre, rivolgersi al più vicino Compartimento di Polizia Postale e delle Comunicazioni (è allegato al presente documento l'elenco dei numeri utili per la segnalazione e delle relative competenze), con l'obiettivo di ottenere la rimozione del materiale e il blocco della sua diffusione. Esso è anche più agevolmente contattabile direttamente dalle Forze dell'Ordine più vicine a cui ci si dovesse rivolgere.

I docenti, sempre con la supervisione del Dirigente Scolastico, stabiliscono, a seconda dei casi, se è più opportuno convocare tutti i genitori per un confronto congiunto (mantenendo l'anonimato di vittime e bulli) o se è meglio un incontro separato. Durante i colloqui con i genitori del bullo, bisogna però avvertirli delle possibili **conseguenze disciplinari (e, se ultraquattordicenne, penali)** delle sue azioni, se accertate. **Chi compie atti di bullismo e cyberbullismo è, infatti, responsabile di reati penali e danni civili:** 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** (art. 612), **danneggiamento** (art. 635). Nei casi più gravi, basta la denuncia ad un organo di polizia o all'autorità giudiziaria per attivare un procedimento penale (per esempio, lesioni o minacce gravi e molestie); negli altri casi, la denuncia deve contenere la richiesta che si proceda penalmente contro l'autore di reato ultraquattordicenne (querela). Nei confronti del minore ultra-quattordicenne autore della condotta di bullismo telematico, per non coinvolgerlo (insieme alla vittima) in procedimenti penali, se non vi sono reati perseguibili d'ufficio, può essere, tuttavia, presentata al Questore (presso qualunque ufficio di polizia) un'istanza di ammonimento che avrà effetto fino alla maggiore età. **Nondimeno, è sempre consigliabile prima cercare di risolvere il caso attraverso le azioni educative.**

La principale azione è, naturalmente, dare il massimo sostegno alla vittima, incoraggiandola a chiedere aiuto, e, una volta contattati i genitori, valutare con loro se necessita di sostegno neuropsichiatrico.

Ma il sostegno deve essere sempre dato anche al bullo e la gestione del caso in classe deve includere azioni a supporto di quest'ultimo: si può stabilire un programma di lavoro che coinvolga tutto il gruppo classe (le attività proposte sul sito del progetto Generazioni Connesse sono numerose e varie, e includono conversazioni guidate e simulazioni), invitando tutti alla comprensione e all'accoglienza (e non all'oppositività o all'evitamento) ogni volta che emergano forme di aggressività, intervenendo con gesti e parole che aiutano il bullo a gestire meglio le proprie azioni ed emozioni e a comprendere che ogni forma di sopraffazione non è accettabile.

È sempre necessario predisporre, quindi, **percorsi formativi** di cui deve beneficiare **l'intero gruppo classe, ribadendo, ogni volta che ci si imbatta in un caso, le regole della sicurezza online e offline e i principi della e-policy d'istituto, conversando in maniera anonima del caso per sensibilizzare i compagni e le compagne, per far loro comprendere la sofferenza della vittima e il danno "ingiusto" che ha subito, per portarli al riconoscimento della gravità dell'accaduto, per combattere l'indifferenza e responsabilizzarli riguardo alle forme "passive" di partecipazione.**

Laddove ritenuto proficuo, il supporto individuale per la vittima e per il bullo può includere attività presso centri di aggregazione giovanile territoriali.

Se si dovesse riscontrare, invece, l'uso di **materiale pedopornografico** è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it, alla sezione **Hotline o Stopit di Save the children**. Questa consente la rimozione del materiale, nonché le attività investigative finalizzate ad identificare chi lo possiede, chi lo diffonde e chi lo produce; ma, soprattutto, consente di identificare i minori abusati presenti nelle immagini e/o video, la fine dell'abuso e l'attivazione del supporto necessario al minore abusato.

Se si ravvisa un rischio per il benessere psicofisico delle persone minorenni coinvolte nella visione di questi (e altri) contenuti inadeguati, sarà anche opportuno rivolgersi ai servizi socio-sanitari del territorio di appartenenza per il necessario supporto psicologico o neuropsichiatrico.

Se, invece, **una studentessa o uno studente della scuola dovesse essere direttamente vittima o testimone in casi di reato di pedopornografia online, anche in sede di raccolta di sommarie informazioni,** il docente deve tenere presente che è **necessaria la presenza di una persona esperta in psicologia o psichiatria infantile (Legge 172 del 2012, art. 351).**

Come nei casi di cyberbullismo, anche in questi casi e in una possibile situazione di **adescamento online (grooming)** che coinvolgesse un/a bambino/a o adolescente (manipolati online dagli adulti per indurli a instaurare una relazione intima), sarà necessario che **il supporto utilizzato dalla persona minorenne non venga più toccato** (ad esempio: non bisogna sostituirsi al bambino/a e/o adolescente e non bisogna rispondere al suo posto). Contestualmente, sarà opportuno rivolgersi tempestivamente ad un presidio di Polizia.

Possono, inoltre, verificarsi casi in cui studentesse e studenti in Rete e nelle chat si imbattano **nell'istigazione al suicidio, all'autolesionismo, all'anoressia e/o alla bulimia.** In tutti questi casi, si dovrà valutare, a seconda del livello di rischio, quale struttura contattare per affrontare il problema. In situazioni di emergenza si farà riferimento ai presidi di pronto soccorso **(118) e poi alla Polizia Postale e delle Comunicazioni (nel caso l'intento sia espresso attraverso la Rete).** Per la valutazione e gestione in una situazione non di emergenza del rischio legato alla possibile messa in atto di tentativi di suicidio o autolesionismo e/o di altre situazioni di disagio, è opportuno (sempre dopo aver effettuato la procedura di segnalazione e averlo comunicato anche alla famiglia), **rivolgersi direttamente alle strutture preposte per offrire il necessario supporto socio-sanitario.**

Se si rilevano casi di **dipendenza da Internet e/o dai videogiochi** (i cui contenuti potrebbero tra l'altro essere violenti o non adatti all'età), è sempre opportuno valutare con la famiglia l'intervento di uno specialista. Qualora si sia anche rilevato l'uso da parte di una persona minorenne di un **gioco d'azzardo online**, è opportuno rivolgersi al più vicino Compartimento di Polizia Postale e delle Comunicazioni, al fine di segnalare l'accessibilità dei siti che gestiscono i giochi, anche considerando che potrebbero essere state utilizzate le credenziali di persone adulte per accedervi.

Infine, i docenti (così come i genitori e le studentesse e gli studenti) che si trovano in dubbio sulla gestione di casi specifici, possono sempre rivolgersi alla helpline di Telefono Azzurro (1.96.96), per avere il parere e il consiglio di esperti. La scuola dà inoltre a tutti gli attori coinvolti una risposta integrata, grazie alla presenza di un docente referente per il cyberbullismo, di un animatore digitale e a collaborazioni specifiche con le Forze dell'Ordine e con l'ASL.

ISTITUTO COMPRENSIVO STATALE "N. CORTESE" CASORIA (NA)

Il Dirigente Scolastico
Prof. Giuseppe Esposito

Delibera C.d.I. n. 2 del 12/4/2018
Delibera Collegio docenti n. 2 del 26/4/2018

Elizabetta Cerino
(ANIMATORE DIGITALE)

(REFERENTE CYBERBULLISMO)

Allegato A: Procedure operative per la prevenzione e rilevazione dei casi

Come prevenire:

Consigli da dare alle studentesse e agli studenti:

Evitare di diffondere in Rete informazioni personali (come l'indirizzo di casa o la scuola che si frequenta); proteggere i propri dati personali, creando password complesse e non rivelandole a terzi, nonché controllando le impostazioni della privacy, se si utilizzano social network; limitare l'abitudine di postare e condividere in maniera eccessiva e chiedere agli amici il permesso esplicito di postare immagini in cui compaiono; evitare di postare immagini personali e intime; usare la webcam in maniera appropriata; non fidarsi ciecamente delle persone conosciute online e parlare con persone vicine di situazioni che creano disagio online; usare videogiochi educativi e sicuri (e mai giocare d'azzardo); informarsi in rete con senso critico.

Per quanto concerne, in particolare, il cyberbullismo, alle studentesse e agli studenti viene poi insegnato a: ***non cancellare le prove se sono vittime di fenomeni di cyberbullismo; bloccare chi infastidisce; parlare dei propri problemi con chi ci si fida; rispettare gli amici virtuali come quelli reali; non inviare messaggi violenti diretti ad accendere battaglie verbali (flaming) e/o messaggi offensivi, finalizzati a ferire (harassment); non danneggiare la reputazione degli altri (denigrazione); non spacciarsi per qualcun altro (impersonation); non rivelare informazioni private altrui (exposure e/o trickery); non escludere una persona da un gruppo online; non molestare e perseguitare online (cyberstalking).***

Attività di prevenzione:

- l'intera comunità scolastica partecipa attivamente ai percorsi di educazione ai diritti e doveri nell'uso delle nuove tecnologie e all'uso consapevole della Rete e di prevenzione dei comportamenti a rischio online, che vengono organizzati dalla scuola, anche mediante la promozione di un ruolo attivo degli studenti e delle studentesse in attività di **peer education**;
- i docenti in classe propongono le attività trasversali alle discipline del curricolo proposte dal Progetto *Generazioni Connesse o altre iniziative idonee alla prevenzione dei disagi causati da un utilizzo inadeguato o poco sicuro della Rete,* **lavora con la classe sul clima** e propone attività finalizzate allo sviluppo dell'empatia e al riconoscimento delle emozioni (proprie e altrui), nonché alla promozione dell'educazione civica (anche digitale). Informa gli alunni/e su ciò che dice la **legge italiana** sul cyberbullismo.

Come rilevare:

Attraverso l'osservazione sistematica, le conversazioni in classe, i temi somministrati, i questionari, lo sportello d'ascolto, le cassette postali (e altri eventuali strumenti di rilevazione scelti dai docenti in base alla classe);

se il docente sospetta **che stia accadendo un fenomeno di disagio legato all'uso della Rete tra gli alunni/e della propria classe:**

- condivide con il docente coordinatore di classe, con il referente per il cyberbullismo (in particolare, se il caso è riferibile a un episodio di bullismo e/o cyberbullismo) e con l'animatore digitale (in particolare, se necessita di supporto informatico specialistico);
- dialoga con i colleghi/e del Consiglio di Classe per confrontarsi e condividere le sue preoccupazioni;

- valuta con loro le possibili strategie di intervento e, se è il caso, il Dirigente Scolastico è avvisato tempestivamente;
- attiva percorsi educativi specifici;
- raccoglie le informazioni, ascoltando i ragazzi e monitorando ciò che accade;
- cerca di capire il livello di diffusione dell'episodio a livello di istituto;
- parla in classe del cyberbullismo e delle sue conseguenze (senza nominare gli alunni che sospetta coinvolti) e suggerisce alle studentesse e agli studenti di **chiedere aiuto** per situazioni di questo tipo.

In caso di dubbio su come procedere o interpretare quello che sta accadendo, può chiedere, in qualsiasi momento, una consulenza telefonica alla **Helpline** del progetto Generazioni Connesse, al numero gratuito **1.96.96.**

Allegato B: Procedure operative per la gestione dei casi

1- Gli alunni e i casi non sono tutti uguali, per cui il vademecum qui proposto è un percorso indicativo (in cui **i docenti devono essere sempre guidati dal superiore interesse dei minori coinvolti).**

L'intervento, seppur tempestivo, deve essere ***condiviso con il coordinatore di classe e con il Dirigente Scolastico (e, nei casi di cyberbullismo, con il docente referente)*** e con **l'animatore digitale** (se si necessita di supporto informatico specialistico), *tenendo conto: dell'unicità degli alunni/e coinvolti/e nella situazione di difficoltà; del tipo di famiglia da cui provengono (se è presente e partecipe e se ha le risorse per affrontare la problematica); del clima in classe e del contesto sociale; se gli alunni/e coinvolti/e hanno una rete di amici che possano supportarli/e; se necessitano del supporto di servizi e istituzioni extra-scolastici.*

2- Differenziare i casi avvenuti a scuola da quelli avvenuti in ambito extra-scolastico.

3- Comportamenti a rischio avvenuti in orario extra-scolastico (di cui la scuola è venuta a conoscenza):

a. riferire il caso al coordinatore della classe (e, se rientra nei casi, al referente per il cyberbullismo) e confrontarsi con i colleghi/e del Consiglio di Classe;
b. compilare la scheda di segnalazione interna e informare i genitori degli alunni interessati (in particolare, nei casi di cyberbullismo, a cura del Dirigente Scolastico);
c. attivare, in base alla gravità dei casi e con la supervisione del Dirigente Scolastico, servizi e istituzioni extra-scolastici.

4- Per segnalare **comportamenti a rischio avvenuti a scuola**:

a. riferire il caso al coordinatore della classe e confrontarsi con i docenti del Consiglio di Classe;
b. in base alla gravità:

- **infrazioni lievi** (come il mancato spegnimento intenzionale e/o l'utilizzo del cellulare senza l'autorizzazione del docente oppure non per l'attività didattica prevista):
- comunicare verbalmente l'accaduto ai genitori degli alunni interessati;
- annotare sul registro elettronico e, se il comportamento è reiterato, stabilire con il Dirigente Scolastico eventuale sanzione disciplinare (da uno a tre giorni e di carattere educativo e con finalità utili alla comunità scolastica).

- **casi gravi**, come la produzione di immagini, audio e/o video non autorizzata, i casi di bullismo e cyberbullismo (e, cioè, **forme di prevaricazione e di oppressione reiterate nel tempo, perpetuate da una persona o da un gruppo nei confronti dei più deboli, offline e/o online**), la frequentazione di siti e chat pro-suicidio, pro-anoressia, pro-bulimia, pro-autolesionismo, la dipendenza da Internet e dai videogiochi:

- compilare la scheda di segnalazione interna (nei casi di cyberbullismo) e comunicare al coordinatore di classe;
- convocare un Consiglio di classe straordinario alla presenza del Dirigente e redigere il relativo verbale;
- segnalare alle famiglie (a cura del Dirigente Scolastico), mediante comunicazione scritta controfirmata per presa visione;
- attivare le procedure secondo i casi (interventi abilitativi; sostegno psicologico; psicoterapia individuale e/o di gruppo, segnalazione al Garante e/o alle Forze dell'Ordine);
- in casi di *cyberbullismo*, acquisire il racconto dei fatti e, se possibile, tutte le informazioni relative ai file che sono stati pubblicati o diffusi (contenuto, modalità di diffusione), con orari e indirizzi Internet, e rivolgersi al docente referente per il cyberbullismo (le azioni, in questo caso, vanno da questi annotate sul relativo diario di bordo) e con l'animatore digitale (se si necessita di supporto informatico specialistico);
- convocare, se ritenuto opportuno, tutti i genitori degli alunni/e e parlare dell'accaduto (in forma anonima);
- attivare percorsi di formazione aggiuntivi per tutta la classe;
- stabilire eventuale sanzione disciplinare (come da regolamento, in base alla gravità e alla continuità dei casi, da uno e fino a quindici giorni, ma di carattere educativo e di utilità per la comunità scolastica).

- casi gravi che includono gli estremi del reato (come: furto di identità, cyberbullismo nel caso di cyberstalking, commercio on-line nel caso di clonazione di carta di credito, pedopornografia on-line, adescamento online, gioco d'azzardo on-line, sexting, lesioni, molestie e/o minacce gravi):
- compilare la scheda di segnalazione interna e informare tempestivamente il coordinatore, il referente per il cyberbullismo e il Dirigente Scolastico;
- segnalare alle autorità competenti (a cura del Dirigente);
- convocare un Consiglio di classe straordinario alla presenza del Dirigente;
- redigere il relativo verbale;
- segnalare alle famiglie (a cura del Dirigente Scolastico, nei casi di cyberbullismo), anche mediante comunicazione scritta da far firmare per presa visione;
- attivare le procedure secondo i casi (interventi abilitativi; sostegno psicologico; psicoterapia individuale e/o di gruppo);
- attivare percorsi di formazione aggiuntivi per tutta la classe e colloqui con il minorenne autore per cercare di responsabilizzarlo e recuperarlo al rispetto dell'altro, aiutarlo a capire le conseguenze delle sue azioni, la responsabilità giuridica – penale e civile – e il danno "ingiusto" che il suo comportamento può aver causato, anche se non intenzionalmente;
- stabilire sanzioni disciplinari (come da regolamento, in base alla gravità dei casi, fino a quindici giorni, con finalità educative e utili alla comunità scolastica).

Infine, i docenti (così come i genitori e le studentesse e gli studenti) che si trovano in dubbio sulla gestione di casi specifici, possono sempre rivolgersi alla helpline di Telefono Azzurro (1.96.96), per avere il parere e il consiglio di esperti. La scuola dà, inoltre, a tutti gli attori coinvolti una risposta integrata, grazie alla presenza di un docente referente per il cyberbullismo, di un animatore digitale e a collaborazioni specifiche con le Forze dell'Ordine e con l'ASL.

Allegato C: MODULO PER LA SEGNALAZIONE DI CASI DI CYBERBULLISMO

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:

FOLLOW-UP DEI CASI

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

SCHEMA RIEPILOGATIVO DEI CASI

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?		

© All rights reserved Generazioni connesse 2017

Allegato D: Numeri utili per la segnalazione dei casi.

Il progetto Generazioni Connesse (www.generazioniconnesse.it) mette a disposizione una serie di servizi che si possono consultare in caso di dubbi riguardo alla rilevazione e alla gestione dei casi:

- N° verde offerto da Telefono Azzurro: 1.96. 96;
- www.stop-it.it di SAVE THE CHILDREN (per materiale pedopornografico).

Ogni cittadino può inoltre rivolgersi alle Forze dell'ordine più vicine e/o ai Servizi e alle Agenzie sotto riportate per rappresentare la propria situazione che riguardi problematiche collegate all'uso improprio di internet:

- **Corecom** (Comitato Regionale per le Comunicazioni: Centro Direzionale Isola, F/8 80142 – Napoli; 081.7783804 – 3805 corecomcampania@consiglio.regione.campania.it www.consiglio.regione.campania.it/corecom/jsp/): *svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.*

- **Ufficio Scolastico Regionale** Via Ponte della Maddalena, 55 80142 – Napoli, 081.5576111; direzione-campania@istruzione.it; www.campania.istruzione.it/home/home.shtml): *supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di internet. Si occupa, in particolare, dei* ***casi di cyberbullismo.***

- **Polizia Postale e delle Comunicazioni** (Compartimento Polizia di stato e delle comunicazioni; Via delle Rep. Marinare, 495 – Napoli - 081.2433001; compartimento.polposta.na@pecps.poliziadistato.it; www.commissariatodips.it/): *accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della rete e che includono gli estremi del reato (furto di identità, cyberbullismo (nel caso di cyberstalking), commercio on-line (nel caso di clonazione di carta di credito), pedopornografia on-line, grooming (adescamento on-line), gioco d'azzardo on-line, sexting).*

- **A.S.L. Napoli 2 Nord - Distretto sanitario n° 43 - Casoria** (Via Alcide de Gasperi, 43, 80026 Casoria NA; 081.8826907; distretto43@aslnapoli2nord.it; distretto43@pec.aslnapoli2nord.it): *fornisce supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in rete.*

- **Garante Regionale per l'Infanzia e l'Adolescenza** (Centro Direzionale Isola, F/8 – Napoli; 081.7783503-843; garanteinfanzia@consiglio.regione.campania.it; www.consiglio.regione.campania.it/garanteinfanzia): *segnala all'autorità giudiziaria i servizi sociali e competenti; accoglie le segnalazioni di presunti abusi; fornisce informazioni sulle modalità di tutela e di esercizio di questi diritti; segnala alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovuti a situazioni ambientali carenti o inadeguate.*

Allegato E: Modello per segnalare episodi di bullismo sul web o sui social network e chiedere l'intervento del Garante per la protezione dei dati personali

Con questo modello si può richiedere al Garante per la protezione dei dati personali di disporre
il blocco/divieto della diffusione online di contenuti ritenuti atti di cyberbullismo
ai sensi dell'art. 2, comma 2, della legge 71/2017 e degli artt. 143 e 144 del d.lgs. 196/2003

INVIARE A
Garante per la protezione dei dati personali
indirizzo e-mail:cyberbullismo@gpdp.it

IMPORTANTE -La segnalazione può essere presentata direttamente da un chi ha un'età maggiore di 14 anni o da chi esercita la responsabilità genitoriale su un minore.

CHI EFFETTUA LA SEGNALAZIONE?

(Scegliere una delle due opzioni e compilare TUTTI i campi)

Mi ritengo vittima di cyberbullismo e **SONO UN MINORE CHE HA COMPIUTO 14 ANNI**	Nome e cognome Luogo e data di nascita Residente a Via/piazza Telefono E-mail/PEC
Ho responsabilità genitoriale su un minore che si ritiene vittima di cyberbullismo	Nome e cognome Luogo e data di nascita Residente a Via/piazza Telefono E-mail/PEC **Chi è il minore vittima di cyberbullismo?** Nome e cognome Luogo e data di nascita Residente a Via/piazza

IN COSA CONSISTE L'AZIONE DI CYBERBULLISMO DI CUI TI RITIENI VITTIMA?

(indicare una o più opzioni nella lista che segue)

pressioni

aggressione

molestia

ricatto

ingiuria

denigrazione

diffamazione

furto d'identità *(es: qualcuno finge di essere me sui social network, hanno rubato le mie password e utilizzato il mio account sui social network, ecc.)*

alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali *(es: qualcuno ha ottenuto e diffuso immagini, video o informazioni che mi riguardano senza che io volessi, ecc.)*

qualcuno ha diffuso online dati e informazioni (video, foto, post, ecc.) per attaccare o ridicolizzare me, e/o la mia famiglia e/o il mio gruppo di amici

QUALI SONO I CONTENUTI CHE VORRESTI FAR RIMUOVERE O OSCURARE SUL WEB O SU UN SOCIAL NETWORK PERCHE' LI CONSIDERI ATTI DI CYBERBULISMO?

(Inserire una sintetica descrizione – **IMPORTANTE SPIEGARE DI COSA SI TRATTA**)

_____

_____

_____

_____

_____

DOVE SONO STATI DIFFUSI I CONTENUTI OFFENSIVI?

sul sito internet [è *necessario indicare l'indirizzo del sito o meglio la URL specifica*]

_____

su uno o più social network[*specificare su quale/i social network e su quale/i profilo/i o pagina/e in particolare*]_____

altro*[specificare*]_____

Se possibile, allegare all'e-mail immagini, video, *screenshot* e/o altri elementi informativi utili relativi all'atto di cyberbullismo e specificare qui sotto di cosa si tratta.

1) _____
2) _____
3) _____

HAI SEGNALATO AL TITOLARE DEL TRATTAMENTO O AL GESTORE DEL SITO WEB O DEL SOCIAL NETWORK CHE TI RITIENI VITTIMA DI CYBERBULLISMO RICHIEDENDO LA RIMOZIONE O L'OSCURAMENTO DEI CONTENUTI MOLESTI?

Si, ma il titolare/gestore non ha provveduto entro i tempi previsti dalla Legge 71/20017 sul cyberbulllismo *[allego copia della richiesta inviata e altri documenti utili]*;

No, perché non ho saputo/potuto identificare chi fosse il titolare/gestore

HAI PRESENTATO DENUNCIA/QUERELA PER I FATTI CHE HAI DESCRITTO?

Si, presso _____;

No

Luogo, data

Nome e cognome

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

Il Garante per la protezione dei dati personali tratterà i dati personali trasmessi, con modalità elettroniche e su supporti cartacei, per lo svolgimento dei compiti istituzionali nell'ambito del contrasto del fenomeno del cyberbullismo. Il loro conferimento è obbligatorio e in assenza degli stessi la segnalazione/reclamo potrebbe non poter essere istruita. I dati personali potrebbero formare oggetto di comunicazione ai soggetti coinvolti nella trattamento dei dati personali oggetto di segnalazione/reclamo (con particolare riferimento a gestori di siti internet e social media), all'Autorità giudiziaria o alle Forze di polizia ovvero ad altri soggetti cui debbano essere comunicati per dare adempimento ad obblighi di legge. Ciascun interessato ha diritto di accedere ai dati personali a sé riferiti e di esercitare gli altri diritti previsti dall'art. 7 del Codice.