Progetto co-finanziato

POLICY DI E-SAFETY

Istituto Comprensivo Statale A. Caponnetto
Via Socrate 11, 90147 Palermo

A.S. 2020/2021

Data revisione 1	*09.02.2021*
Ratificato	*Consiglio d'Istituto con delibera n. 53 del 28/06/2019*
Approvato	*Collegio Docenti con delibera n.31 del 20/05/2019*
Prossima revisione	*Settembre 2021*

INDICE

1. INTRODUZIONE

1.1 PREMESSA

Lo sviluppo e l'integrazione dell'uso delle "tecnologie dell'informazione e della comunicazione" (TIC) nella didattica pone nuove attenzioni dal punto di vista del loro uso sicuro e consapevole.
E' compito dell'intera comunità scolastica, genitori inclusi, garantire che gli studenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato. In questo quadro si inserisce la necessità di dotare la scuola di una propria Policy di E-safety, nell'ottica della promozione dell'uso consapevole delle tecnologie digitali e della gestione delle infrazioni attraverso il monitoraggio continuo della Policy e la sua integrazione con il Regolamento d'Istituto. Obiettivo del presente documento è quello di educare e sensibilizzare l'intera comunità scolastica all'uso sicuro e consapevole di INTERNET in conformità con le "Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e cyberbullismo" elaborate dal Ministero dell'Istruzione e della Ricerca in collaborazione con il Safer Internet Center per l'Italia, programma istituito dalla Comunità Europea.
La capacità di partecipare in modo costruttivo e consapevole alle comunità on line e ai network virtuali costituisce un prerequisito fondamentale per partecipare in modo attivo alla società della conoscenza e dell'informazione. Alla diffusione dei nuovi media e degli strumenti del web 2.0 si accompagna infatti l'emergere di nuove opportunità di partecipazione civica e sociale (e-engagement, e-inclusion), che richiedono capacità comunicative e socio-relazionali adeguate.
E' fondamentale quindi conoscere come ci si comporta in queste comunità, quali regole vanno rispettate e quali ruoli e responsabilità hanno i soggetti che vi partecipano. La scuola, nel farsi carico della formazione globale dell'individuo nella fase evolutiva, deve individuare in maniera chiara e inequivocabile ruoli e responsabilità di ciascuno degli attori del percorso formativo

1.2 SCOPO DELLA POLICY

La Policy di e-safety è un documento, autoprodotto dalla scuola, con l'obiettivo di esprimere:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

1.3 STRUMENTI TECNOLOGICI A SERVIZIO DELLA SCUOLA

La scuola si avvale di diversi strumenti informatici a sostegno sia delle funzioni amministrative che di quelle didattiche. Il software Argo a cui possono accedere Dirigente, il DSGA e il personale amministrativo offre supporto alla gestione amministrativa delle utenze, venendo incontro alle nuove esigenze di integrazione dei servizi e dematerializzazione che sono uno degli obiettivi delle pubbliche amministrazioni. Grazie all'implementazione costante del proprio sito internet, la scuola comunica al territorio le proprie iniziative, garantendo l'accesso alla documentazione necessaria ad una partecipazione attiva da parte degli utenti in modo chiaro e tempestivo. Il registro elettronico "Didup" di Argo supporta i docenti nella gestione quotidiana delle proprie attività didattiche, rendendo le operazioni di valutazione e di scrutinio più efficienti. Il registro contiene anche diversi spazi per l'archiviazione della documentazione dei docenti (verbali, programmazioni) secondo le procedure illustrate nel Piano di DDI elaborato dall'Istituto. L'Istituto ha attualmente in uso G suite for Education avendo registrato un proprio dominio (@iccaponnetto.edu.it). All'interno di quest'area vengono create classi virtuali (Google Classroom) e gli studenti e i docenti possono comunicare in modo sicuro e protetto. All'interno di drive sono state create repository per lo scambio di materiali e documenti da parte dei docenti. La scuola, intercettando tutte le opportunità di finanziamento rese disponibili dalle amministrazioni, ha implementato le tecnologie presenti in tutti i suoi ordini di scuola, con l'obiettivo di adeguare i propri strumenti e i propri servizi ai bisogni dell'utenza.

Attualmente l'istituto è dotato di: due aule informatiche con LIM e postazioni pc (plesso scuola secondaria di primo grado e plesso scuola primaria in via Limone), un laboratorio linguistico con LIM e postazioni pc (scuola secondaria di primo grado) per la realizzazione di attività laboratoriali. Due aule della scuola primaria del plesso centrale, 1 aula della scuola primaria in Via Limoni e 6 aule della scuola secondaria sono dotate di LIM. Le strumentazioni sono state recentemente potenziate con dotazioni di n 16 notebook, 11 chiavette per la connettività ed n 1 licenza per il symwriter acquisiti durante l'emergenza Covid con fondi specifici. E', inoltre, presente attrezzatura dedicata ai ragazzi con Bisogni Educativi Speciali e software specifici per l'apprendimento. Tutte le aule della scuola sono sono collegate ad internet attraverso il Wifi.

1.4 RUOLI E RESPONSABILITA'

Affinché l'E-policy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, s'impegni nell'attuazione e promozione di essa

RUOLO	RESPONSABILITA'
La Dirigente Scolastica	• responsabilità di una adeguata informazione del personale sui ruoli da svolgere per la sicurezza on-line e per la formazione di altri colleghi; • titolarità sul del trattamento dei dati (PPO); • garantire che la scuola utilizzi un Internet Service filtrato approvato, conforme ai requisiti di legge vigenti ; • essere a conoscenza delle procedure da seguire in caso di infrazione della E–Safety Policy; • ruolo di primo piano nello stabilire e rivedere la E-Safety Policy; • ricevere relazioni di monitoraggio periodiche della sicurezza online da parte del responsabile; • garantire che vi sia un sistema in grado di monitorare il personale di supporto che svolge le procedure di sicurezza online interne
Il Direttore dei servizi generali e amministrativi	• assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni; • garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.
L'Animatore Digitale ed il suo Team	• pubblicare la E-Safety Policy sul sito della scuola; • diffondere la E- Safety Policy attraverso power point e schede semplificative; • garantire che tutti i dati relativi agli alunni pubblicati sul sito siano sufficientemente tutelati; • promuovere azioni di sensibilizzazione/formazione per un uso consapevole delle nuove tecnologie e della rete; • promuove l'uso delle nuove tecnologie nella didattica; • coordina la partecipazione ad eventi inerenti lo sviluppo delle competenze digitali degli utenti della scuola; • mettere in atto norme, procedure e regolamenti per il corretto uso delle tecnologie al servizio della didattica;

Il referente per il bullismo e cyberbullismo	• mettere in atto i passaggi riportati nella procedura per il trattamento di casi evidenti/sospetti legati al Cyber-bullismo interagendo con i diversi attori a seguito di opportune valutazioni
I docenti	• Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti: • informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento; • garantire modalità di utilizzo corretto e sicuro delle TIC e di internet (anche da parte degli alunni) • assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente; • nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei; • comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni • sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
Gli alunni	• Il ruolo degli alunni include i seguenti compiti: • essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti; • avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali; • comprendere l'importanza di adottare buone pratiche di sicurezza on-line (rapportate al grado di maturità e all'età degli studenti) quando si utilizzano le tecnologie digitali per non correre rischi; • adottare condotte rispettose degli altri anche quando si comunica in rete; • esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

I genitori	Il ruolo dei genitori degli alunni include i seguenti compiti: • 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 del telefonino in generale.

1.5 CONDIVISIONE E COMUNICAZIONE DELLA POLICY ALL'INTERA COMUNITÀ SCOLASTICA

L'E-policy, approvata dal Collegio dei Docenti e dal Consiglio di Istituto, viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola con uno spazio dedicato alle tematiche del bullismo e del cyberbullismo.
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

I docenti inoltre presenteranno agli alunni e alle famiglie questa Policy e saranno previste alcune lezioni sulle buone pratiche, per un utilizzo sicuro del digitale. Il contenuto della Policy sarà condiviso all'interno dell'intera comunità scolastica, attraverso comunicazioni da effettuare nel corso dei Consigli di Intersezione, dei Consigli di Interclasse, dei Consigli di Classe, del Collegio Docenti e del Consiglio di Istituto, anche con la presenza dei genitori rappresentanti, che potranno accedere a materiali, resi disponibili sul sito web della scuola.

1.6 GESTIONE DELLE INFRAZIONI ALLA POLICY

Le infrazioni alla policy possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni

oppure possono essere segnalate da alunni e genitori a docenti/ATA, referente cyberbullismo, vicario della Dirigente e al Dirigente scolastico stesso. Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso.

Il nostro istituto possiede una rete per l'accesso ad internet dotata di filtri che impediscono l'accesso a siti non adatti ai minori (black list); sicurezza per la navigazione. La scuola monitora periodicamente l'utilizzo di internet e nel caso si trovi materiale indesiderato prende tutte le precauzioni possibili per assicurare la sicurezza nell'uso delle tecnologie informatiche.
Tuttavia, a causa della scala internazionale collegata ai contenuti Internet, la disponibilità di tecnologie mobili e velocità di cambiamento, non è possibile garantire che il materiale non idoneo apparirà mai su un computer della scuola o dispositivo mobile. Né la scuola né l'autorità locale possono accettare la responsabilità per il materiale accessibile, o le conseguenze di accesso a Internet.

1) Disciplina degli alunni

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

- un uso della rete per giudicare, infastidire o impedire, in modo persistente, a qualcuno di esprimersi o di partecipare;
- l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono; l'invio o la condivisione di immagini intime o troppo spinte;
- il collegamento a siti web, nell'orario scolastico, non autorizzati dai docenti;
- L'utilizzo, non autorizzato o comunicato ai docenti, dello smartphone in orario scolastico (utilizzando messaggeria, video, audio o foto).

Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo dell'alunno. Infatti più gli alunni sono piccoli, più i comportamenti "da correggere" sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, che devono essere compresi e orientati proprio dagli educatori, nella prospettiva del raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno.
Sono previsti pertanto da parte dei docenti provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento, quali:

- il richiamo verbale;
- il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);
- il richiamo scritto con annotazione sul diario;
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente scolastico.

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza attraverso la

partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni.

2) Disciplina del personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet sono diverse e alcune possono determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli alunni:

- un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite 'installazione di software o il salvataggio di materiali non idonei;
- un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- una carente istruzione preventiva degli alunni sull'utilizzazione corretta e responsabile delle tecnologie digitali e di internet;
- una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale. Il Dirigente scolastico può 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, conservandone una copia per eventuali successive investigazioni. Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

3) 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 da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico.

Le situazioni familiari meno favorevoli sono:

- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai;
- 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 senza una periodica condivisione o controllo dei contenuti;
- la mancanza di adeguata conoscenza che la responsabilità dei contenuti dello smartphone dei minori è sempre ascrivibile ai genitori/tutori;
- assoluto disinteresse sui contenuti dello smartphone dei propri figli;
- 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.

Denunce di bullismo online saranno trattate in conformità con la legge attuale, 29/05/2017 n° 71, G.U. 03/06/2017 recante "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo".

1.7 MONITORAGGIO DELL'IMPLEMENTAZIONE DELLA POLICY E SUO AGGIORNAMENTO

Il Dirigente Scolastico è responsabile dell'implementazione della E-Safety Policy all'interno dell'Istituto. L'Animatore Digitale, il Team digitale, il Referente per il Bullismo e il Cyberbullismo, collaborano con il Dirigente Scolastico, per la revisione e l'aggiornamento del documento

La E-Safety Policy sarà riesaminata annualmente o quando si verifichino cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola e/o la normativa di riferimento. Tutte le modifiche della Policy saranno sempre discusse in dettaglio nella seduta collegiale dei docenti. Nell'ambito della revisione della Policy, tutte le informazioni e le revisioni saranno memorizzate per eventuali controlli.

1.8 INTEGRAZIONE DELLA POLICY CON REGOLAMENTI ESISTENTI

Il presente documento si integra con il Piano Triennale dell'Offerta Formativa ed è allegato al Regolamento di Istituto.

Va ad integrare tale Regolamento costituendo la sezione relativa all' uso delle nuove tecnologie, dei nuovi ambienti di apprendimento e metodologie come "Regolamento per l'uso delle risorse tecnologiche e di rete".

Le istruzioni contenute in questi allegati vanno sostituite e/o integrate con le norme contenute all'interno del Regolamento Covid che è stato approvato dal Consiglio di Istituto, valido per l'a.s. 2020-21 ed al Piano Scolastico per la Didattica Digitale Integrata.

2. FORMAZIONE E CURRICOLO

Il nostro Istituto condivide le linee indicate nel Piano Nazionale Scuola Digitale (PNSD). Esse danno come indirizzo l'intento di modificare gli ambienti di apprendimento per rendere l'offerta formativa coerente con i cambiamenti della società della conoscenza e con le esigenze e gli stili cognitivi delle nuove generazioni. Si ricorda il D.M. 851 del 27 ottobre 2015, in attuazione dell'art.1, comma 56 della legge 107/2015, che ne prevede l'attuazione al fine di:

- migliorare le competenze digitali degli studenti anche attraverso un uso consapevole delle stesse;
- implementare le dotazioni tecnologiche della scuola al fine di migliorare gli strumenti didattici e laboratoriali ivi presenti;
- favorire la formazione dei docenti sull'uso delle nuove tecnologie ai fini dell'innovazione didattica;
- individuare un Animatore Digitale ed un team per l'innovazione digitale che supporti ed accompagni adeguatamente l'innovazione didattica, nonché l'attività dell'animatore Digitale;
- partecipare a bandi nazionali ed europei per finanziare le suddette iniziative;

2.1 CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI

Le Nuove Indicazioni Nazionali del 2012 in raccordo con il programma europeo "Competenze chiave per un mondo in trasformazione" prevedono che al termine del primo grado di istruzione lo studente possegga buone competenze digitali e sappia usare 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.
"La responsabilità è l'atteggiamento che connota la competenza digitale" - così come viene citato nel Documento a cura del Comitato Scientifico Nazionale per le Indicazioni Nazionali per il curricolo della scuola dell'infanzia e del primo ciclo di istruzione del 22/02/2018. I ragazzi, anche se definiti nativi digitali, spesso non sanno usare le macchine, utilizzare i software fondamentali, fogli di calcolo, elaboratori di testo, navigare in rete per cercare informazioni in modo consapevole. Tuttavia, come suggeriscono anche i documenti europei sulla educazione digitale, le abilità tecniche non bastano. La maggior parte della competenza è costituita dal sapere cercare, scegliere, valutare le informazioni in rete e nella responsabilità nell'uso dei mezzi, per non nuocere a sé stessi e agli altri. In questo senso le TIC (Tecnologie dell'Informazione e della Comunicazione) preparano studentesse e studenti ad un'attiva e consapevole partecipazione ad un mondo in rapida evoluzione nel quale è necessario acquisire abilità e competenze in grado di facilitare l'adattamento dell'individuo ai continui

cambiamenti. Si rende quindi necessario lo sviluppo e la diffusione di una mentalità tecnologica diffusa e precoce, intesa come alfabetizzazione al senso, all'utilizzabilità in contesti dati e per scopi definiti da un lato ed una acquisizione sempre più consapevole di strategie efficaci per il dominio di una macchina complessa che impiega e genera oggetti immateriali dall'altro. Alunne e alunni dovrebbero quindi imparare ad utilizzare le TIC per cercare, esplorare, scambiare e presentare informazioni in modo responsabile, creativo e con senso critico, essere in grado di avere un rapido accesso a idee ed esperienze provenienti da persone, comunità e culture diverse. Alla scuola spetta quindi anche il compito di trovare raccordi efficaci tra la crescente dimestichezza degli adolescenti con le Tecnologie dell'Informazione e della Comunicazione e l'azione didattica quotidiana. Le TIC possono infatti offrire significative occasioni per sviluppare le competenze di comunicazione, collaborazione e problem solving.

2.2 FORMAZIONE DEI DOCENTI SULL'UTILIZZO E L'INTEGRAZIONE DELLE TIC NELLA DIDATTICA

La formazione dei docenti e del personale che opera nella scuola è un importante elemento di qualità nel servizio scolastico; essa rappresenta una leva strategica per lo sviluppo culturale dell'istituzione scolastica, per il necessario sostegno agli obiettivi di cambiamento e per un'efficace politica delle risorse umane. 6 Il comma 124 della Legge n. 107/2015 dispone: "Nell'ambito degli adempimenti connessi alla funzione docente, la formazione in servizio dei docenti di ruolo è obbligatoria, permanente e strutturale. Le attività di formazione sono definite dalle singole istituzioni scolastiche in coerenza con il piano triennale dell'offerta formativa e con i risultati emersi dai piani di miglioramento delle istituzioni scolastiche previsti dal regolamento di cui al decreto del Presidente della Repubblica 28 marzo 2013, n. 80, sulla base delle priorità nazionali indicate nel Piano nazionale di formazione, adottato ogni tre anni con decreto del Ministro dell'istruzione, dell'Università e della ricerca, sentite le organizzazioni sindacali rappresentative di categoria."

L'Istituto riconosce e favorisce la partecipazione del personale ad iniziative promosse sia dalla scuola, dalle Reti di scuole, dall'Amministrazione, sia da quelle scelte liberamente dai docenti, purché coerenti con il piano di formazione. Fondamentale porre attenzione all'uso del TIC nella didattica: un loro utilizzo strutturato e integrato rende gli apprendimenti motivanti, coinvolgenti ed inclusivi e permette al docente di guidare studenti e studentesse nella fruizione dei contenuti online, sempre più importante anche in ambito lavorativo (lavoro di gruppo anche a distanza, confronto fra pari in modalità asincrona).

2.3 FORMAZIONE DEI DOCENTI SULL'UTILIZZO CONSAPEVOLE E SICURO DI INTERNET E DELLE TECNOLOGIE DIGITALI

Coerentemente con quanto previsto dal PNSD, ed in modo particolare con l'azione #28, la nostra Scuola si avvale dell'Animatore Digitale, una figura di sistema, che con il Dirigente scolastico e il D.S.G.A. opera per concretizzare gli obiettivi e le innovazioni del PNSD nella vita scolastica. L'Animatore Digitale è affiancato da un Team per l'Innovazione Digitale che supporta ed accompagna adeguatamente l'innovazione didattica, nonché l'attività dell'Animatore Digitale. Nasce quindi la necessità di una formazione specifica che possa "favorire il processo di digitalizzazione delle scuole nonché diffondere le politiche legate all'innovazione didattica attraverso azioni di accompagnamento e di sostegno sul territorio del piano nazionale scuola digitale" (rif. Prot. n.17791 del 19/11/2015). Anche il percorso della formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet, può prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente, conseguentemente all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi.
La scuola assicura tempestiva e capillare informazione su corsi, convegni e seminari che riguardino tali argomenti, cercando altresì di agevolare il personale che intenda parteciparvi. Infine la scuola può aderire a progetti appositi di formazione presentati da enti e associazioni. La formazione deve avviare, dunque, un concreto processo di feed-back autovalutativo che comporti la revisione delle prassi metodologiche e didattiche adottate e promuova nei docenti la consapevolezza di un nuovo modo di essere educatori ed esploratori del "quotidiano virtuale" degli studenti, spesso inconsapevoli dei pericoli non sempre tangibili della Rete. Innovazione radicale, quindi, per docenti e formatori che impone loro una preparazione specifica per rispondere ai nuovi stili cognitivi e comunicativi degli studenti. Ne scaturisce il ruolo fondamentale che deve assumere la Comunità scolastica nel guidare gli studenti verso la consapevolezza dei propri diritti e doveri di "cittadini virtuali".
La scuola partecipa dal 2017/18 al programma "generazioni connesse" sui cui è disponibile una piattaforma di formazione destinata a tutti i docenti dell'Istituto che vogliano formarsi sull'argomento specifico delle nuove tecnologie.

2.4 SENSIBILIZZAZIONE DELLE FAMIGLIE

Il nostro istituto ha organizzato già negli anni passati incontri aperti alle famiglie e agli studenti con l'associazione "Passe par tout", per sensibilizzare docenti, alunne, alunni e genitori sui temi del bullismo e del cyberbullismo. Anche nei prossimi anni si continuerà ad utilizzare questo approccio per la sensibilizzazione delle famiglie, con incontri che offriranno occasione di confronto e discussione sui rischi rappresentati dall'uso di cellulari, smartphone e chat line senza un'adeguata formazione in

merito ai rischi derivanti da un uso inappropriato di tali dispositivi. Sul sito scolastico saranno resi accessibili i materiali dedicati alle famiglie, alle ragazze e ai ragazzi nella bacheca virtuale del sito di "Generazioni Connesse". La scuola darà inoltre ampia diffusione, tramite pubblicazione sul sito, del presente documento di Policy per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e favorire un'attiva collaborazione tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi a un uso inappropriato del digitale.

3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA E NELLA SCUOLA

La scuola metterà in atto tutte le azioni necessarie per garantire agli studenti l'accesso alla documentazione cercata adottando tutti i sistemi di sicurezza conosciuti per diminuire le possibilità di rischio durante la navigazione. Resta fermo che non è possibile garantire una navigazione totalmente priva di rischi e che la Scuola e gli insegnanti non possono assumersi le responsabilità conseguenti all'accesso accidentale e/o improprio a siti illeciti.

L'infrastruttura e la strumentazione TIC dell'Istituto sono un patrimonio di tutti e vanno utilizzate nel rispetto delle norme contenute nel Regolamento d'Istituto e nei Regolamenti dei singoli laboratori multimediali. I danni causati alle attrezzature saranno a carico di chiunque disattenda i suddetti Regolamenti. La scuola deve considerare l'ambiente on line alla stregua dell'ambiente fisico e valutarne tutti gli aspetti legati alla sicurezza. Per quanto concerne l'hardware la scuola provvede a pianificare interventi periodici di manutenzione.

3.1 ACCESSO AD INTERNET: FILTRI, ANTIVIRUS E SULLA NAVIGAZIONE

L'accesso a Internet è possibile in tutte le aule e nei laboratori d'informatica. Le impostazioni sono definite e gestite dal responsabile dei laboratori ed è in carico a ciascun docente la segnalazione di malfunzionamenti e disservizi, al fine di richiedere, ove necessario, l'intervento di tecnici esterni. I docenti hanno piena autonomia nel collegamento ai siti web nelle postazioni a loro riservate. Relativamente agli alunni che accedono a Internet durante l'attività didattica sono consentiti la navigazione guidata da parte dell'insegnante e la stesura di documenti collaborativi purché sotto il controllo dell'insegnante e nel caso in cui tale attività faccia parte di un progetto di lavoro precedentemente autorizzato.
Nei laboratori informatici e linguistici, sono presenti PC desktop, mentre nelle aule dotate di LIM sono utilizzati soprattutto notebook. Tutti i computer presenti nella scuola sono provvisti di un antivirus. I docenti possono accedere alla rete Internet mediante mobile device personali esclusivamente in modalità wireless. Le alunne e gli alunni possono accedere alla rete Internet con i propri dispositivi, in occasione di attività didattiche e/o formative svolte in classe sotto la responsabilità e la sorveglianza di un insegnante. La rete Internet non può essere utilizzata per scopi vietati dalla legislazione vigente e gli utenti sono direttamente responsabili, civilmente e penalmente, a norma delle vigenti leggi, per ogni attività svolta. È vietato scaricare ed installare

software sui PC e/o mobile device della scuola senza preventiva autorizzazione.

3.2 GESTIONE ACCESSI

La scuola attualmente è dotata di una rete wireless destinata all'utilizzo didattico da parte del corpo docente. I computer portatili non richiedono una password di accesso per l'accensione. L'autenticazione tramite password è prevista solo per il PC presente nel laboratorio informatico. Ogni docente deve, quindi, controllare la strumentazione poiché l'uso del dispositivo è permesso alle alunne e agli alunni solo su autorizzazione dell'insegnante. Ogni docente accede al registro elettronico attraverso una password personale che non può essere comunicata a terzi. Ciascun utente connesso alla rete dovrà rispettare il presente regolamento, tutelare la propria privacy, quella degli altri utenti adulti e delle alunne e degli alunni per evitare la divulgazione di notizie private contenute nelle documentazioni elettroniche cui ha accesso e rispettare la cosiddetta netiquette (insieme di regole, comunemente accettate e seguite da quanti utilizzano Internet e i servizi di rete, che disciplinano il comportamento di un utente nel rapportarsi agli altri utenti attraverso risorse come wiki, newsgroup, mailing list, forum, blog o e - mail). Le alunne e gli alunni dovranno impegnarsi a rispettare le norme di buon utilizzo che la scuola ha redatto.

Accesso al personale amministrativo

Il personale amministrativo accede agli strumenti informatici assegnati attraverso credenziali fornite dal DSGA.

Accesso docenti

Ai docenti è consentito accedere ad Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto previo inserimento di una password di accesso alla rete scolastica. Tale password è comunicata ai docenti che avranno cura di custodirla garantendone la segretezza. Il proprietario delle credenziali è l'unico responsabile delle operazioni svolte con esse. Il docente verificherà la disconnessione del dispositivo utilizzato in aula dalla rete al termine della sua ora di lezione.

Accesso studenti

Il Regolamento di Istituto vieta l'uso del cellulare ad eccezione di specifiche attività didattiche svolte sotto la supervisione del docente che ne autorizza l'uso in byod. In questi casi agli studenti è consentito accedere ad Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto. In questo caso gli alunni utilizzeranno credenziali di accesso attivate con scadenza temporale dalla vicepreside.

E' assolutamente vietato usare pendrive personali a qualunque titolo. Nelle aule multimediali i docenti registrano il proprio accesso, scrivendo su un registro la data e l'orario di utilizzo del

laboratorio. Le postazioni del laboratorio funzionano come stazioni di lavoro e non come archivi. Ogni docente è quindi tenuto ad un controllo della strumentazione in aula poiché l'uso del dispositivo è permesso agli alunni solo su autorizzazione dell'insegnante.

3.3 DISPOSITIVI PERSONALI E REGOLE PER IL BYOD

Per gli studenti: è vietato l'utilizzo di cellulari per l'intera durata delle attività scolastiche. È consentito a tutti gli studenti, in casi specifici concordati con il docente, l'utilizzo di dispostivi elettronici personali per scopi didattici (modalità BYOD, Bring your own device).

Per i docenti: durante l'orario di servizio l'utilizzo di dispostivi elettronici personali è consentito per i soli fini didattici. Il personale della scuola ha facoltà di usare strumenti personali in caso di stretta necessità o nelle pause di lavoro.

Regole per il BYOD: L'azione #6 del Piano Nazionale Scuola Digitale "Politiche attive per il BYOD" (Bring Your Own Device, traduzione: porta il tuo dispositivo) intende garantire a tutti gli studenti una formazione digitale fondata sul saper usare i propri device in modo consapevole. Nel ribadire che l'uso improprio dei dispositivi digitali mobili a scuola è inaccettabile e sanzionato in base a quanto stabilito dal Regolamento di Istituto, si definiscono, in linea con il PNSD, le seguenti regole BYOD per favorire l'attuazione dell'azione #6, garantendone la sicurezza:

- i dispositivi personali - computer portatili, tablet, e-reader, smartphone - possono essere usati a scuola solo per scopi didattici, previa autorizzazione esplicita dell'insegnante e sotto la supervisione dello stesso;
- è severamente vietato usare dispositivi di registrazione audio, videocamere o fotocamere (o dispositivi che li prevedano) per registrare o fare foto in classe senza il permesso dell'insegnante e senza il consenso della persona che viene registrata, videoregistrata, fotografata;
- gli studenti dovranno consegnare i propri dispositivi mobili che verranno custoditi, chiusi in una busta trasparente, in un'apposita scatola
- la scuola non è responsabile della sicurezza dei dispositivi e di eventuali danni o smarrimenti agli studenti è richiesto di caricare il dispositivo a casa; non è consentito ricaricare i dispositivi in aula anche per motivi di sicurezza
- gli studenti devono rispettare la proprietà intellettuale altrui: - non sono ammessi copia e/o plagio di qualsivoglia materiale - non è ammessa la violazione del copyright
- L'Istituto può ispezionare, previa autorizzazione anche verbale del genitore o del tutore, la memoria del dispositivo dello studente, se ritiene che le regole non siano state rispettate.

Ciò comprende registrazioni audio e video, fotografie scattate negli ambienti di pertinenza dell'Istituto e ogni altro materiale che violi la dignità e la privacy altrui.

3.4 E-MAIL

L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. L'eventuale invio o ricevimento di posta a scopi didattici avverrebbe solo su autorizzazione del Dirigente scolastico e operativamente sarebbe svolto dall'assistente amministrativo addetto. La posta elettronica è protetta da antivirus.

La Scuola è dotata di un sito istituzionale (www.icsacaponnetto.edu.it) che prevede un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, avvisi di carattere generale.

3.5 SOCIAL NETWORK

L'istituzione scolastica possiede un profilo YOUTUBE, una pagina FACEBOOK ed un canale TELEGRAM gestito dal personale autorizzato dal Dirigente Scolastico per la pubblicazione di materiali video inerenti attività didattiche svolte dai docenti insieme agli studenti. Il canale telegram viene inoltre utilizzato per comunicazioni rivolte all'utenza.

E' fatto esplicitamente divieto ad alunni, docenti, personale ATA e Genitori di pubblicare immagini, video, commenti su qualunque social network se non ad esclusivo scopo didattico in accordo con quanto previsto nel rispetto della privacy e delle regole relative ai Social Network. Si ricorda che la diffusione di foto/filmati senza il consenso e, comunque, all'insaputa delle persone coinvolte può determinare ricadute di carattere anche penale, come ad esempio la diffamazione. Si invitano pertanto tutti gli studenti a non prelevare o diffondere immagini, video o registrazioni – anche solo audio – non autorizzate, ed eliminare da internet eventuali riferimenti offensivi o comunque illeciti (ed inopportuni) nei confronti dell'Istituto e dei suoi docenti e studenti. Allo stesso tempo, si invitano gli allievi e i genitori a fare un uso prudente dei Social Network, in particolare Facebook e Whatsapp, limitandone l'uso alle sole comunicazioni funzionali, evitando ad ogni modo di esprimere giudizi sull'operato degli altri studenti o del personale della scuola, giudizi che una volta pubblicati comportano sempre una assunzione di responsabilità da parte di chi li ha scritti o anche semplicemente diffusi.

3.6 PIATTAFORME DIDATTICHE E GSUITE FOR EDUCATION

A partire dall'anno scolastico 2020/21 il nostro Istituto ha attivato la G Suite for Education, un insieme di applicativi messi a disposizione da Google per le scuole, al fine di facilitare, sostenere e motivare l'apprendimento attraverso le nuove tecnologie. G Suite è costituita da un insieme di applicazioni. Le principali sono: la posta elettronica (Gmail), i documenti condivisi (Google Drive), il Calendario (Google Calendar), le classi virtuali (Google Classroom), la piattaforma per le videolezioni (Google Meet). Le funzionalità sono le stesse, praticamente identiche a quelle degli account Gmail di tipo privato (a parte Google Classroom), ma la grande differenza è nelle condizioni d'uso: per le G Suite for Education la proprietà dei dati rimane in capo all'utente, con totale protezione della privacy e priva di pubblicità, mentre per gli account privati le possibilità di "intromissione" da parte di Google sono numerose.

In accordo con le linee guida del Piano Nazionale per Scuola Digitale, il nostro Istituto ha creato un dominio @iccaponnetto.edu.it associato alla piattaforma G Suite for Education.

L'account G Suite for Education è attivato per tutti i docenti e gli studenti dell'Istituto i quali riceveranno un account personale gratuito con nomeutente e password per l'accesso ai servizi di base di Google di cui potranno usufruire fino al termine del loro percorso scolastico nel nostro istituto.

Il regolamento G-Suite e l'informativa su G-Suite per i genitori e i tutori sono pubblicati sul sito della scuola (https://www.iccaponnetto.edu.it/index.php/g-suite-for-education) e si integrano alla policy di e-safety.

3.7 PROTEZIONE DEI DATI PERSONALI

L'Istituto Comprensivo "Antonino Caponnetto" rispetta la privacy dei propri utenti e si impegna a proteggere i dati personali che gli stessi conferiscono all'Istituto. In generale, l'utente può navigare sul sito web della scuola senza fornire alcun tipo di informazione personale.

Il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). L'istituto tratta i dati personali forniti dagli utenti in conformità alla normativa vigente.

4. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

4.1 SENSIBILIZZAZIONE E PREVENZIONE

Il rischio online si configura come la possibilità per il minore di:

- commettere azioni online che possano danneggiare se stessi o altri;
- essere una vittima di queste azioni;
- osservare altri commettere queste azioni.

È importante riconoscere questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per arginarli e contenerli, ma è altrettanto importante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano. Ciò è possibile lavorando su aspetti di ampio raggio che possano permettere una riduzione dei fattori di rischio e di conseguenza una minore probabilità che i ragazzi si trovino in situazioni non piacevoli. È importante che abbiano gli strumenti idonei per riconoscere possibili situazioni di rischio e segnalarle ad un adulto di riferimento.

Gli strumenti da adottare per poter ridurre l'incidenza di situazioni di rischio si configurano come interventi di sensibilizzazione e prevenzione.

Nel caso della sensibilizzazione si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.
Nel caso della prevenzione si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.

Le azioni di sensibilizzazione riguarderanno:

- accrescere la consapevolezza nel gruppo target di riferimento circa un determinato tema/bisogno/problema che potrebbe presentarsi in quel gruppo;
- incoraggiare il gruppo a modificare i propri comportamenti rendendoli più funzionali;
- diffondere all'esterno del gruppo di riferimento e quindi tra l'opinione pubblica una certa consapevolezza rispetto all'argomento di interesse;
- facilitare il coinvolgimento di soggetti esterni in modo da mettere insieme diverse idee per

lavorare ad un obiettivo comune;
- favorire la diffusione di informazioni e servizi disponibili all'utilità collettiva (promuovere la conoscenza dell'ePolicy nella comunità scolastica).

Se il problema della "sicurezza" è difficilmente riconducibile esclusivamente all'esistenza in sé di alcuni rischi, più o meno gravi e insidiosi, appare chiaro come le migliori strategie di intervento siano di carattere prevalentemente preventivo.

Le misure di prevenzione comprendono l'integrazione nel curricolo dei temi legati al corretto utilizzo delle TIC e di Internet in quanto, poiché per i nativi digitali le interconnessioni tra vita e tecnologia sono la normalità, essi, pur essendo tecnicamente competenti, tendono a non cogliere le implicazioni dei loro comportamenti.
Come scuola intendiamo per prevenzione un insieme molto ampio di strategie che coinvolgano le famiglie e le forze sociali che operano sul territorio al fine di mettere al proprio centro l'educazione formativa dei ragazzi.
La Scuola ha scelto una politica interna che sia pro-attiva, tesa cioè a creare un ambiente di apprendimento sereno e sicuro in cui sia chiaro sin dal primo giorno di scuola che (cyber)bullismo, prepotenza, aggressione e violenza non sono permessi, in cui ci sia l'apertura necessaria all'incoraggiamento a parlare di sé e dei propri problemi, che stimoli alla partecipazione diffusa di tutta la comunità scolastica nelle azioni finalizzate al contrasto del (cyber)bullismo, che insegni ad interagire in maniera responsabile.
Contrastare il bullismo implica la creazione di una comunità solidale, in cui ogni allievo accetta sia il diritto di vivere una scuola senza violenza, sia la responsabilità di difendere i compagni più vulnerabili. Il coinvolgimento dei coetanei è indispensabile per creare un clima di solidarietà, combattere l'omertà e l'indifferenza, incoraggiare le vittime a chiedere aiuto, sottrarre al bullo i potenziali proseliti.
Diventa quindi importante che l'insegnante, nell'espletamento delle proprie funzioni, aiuti le proprie alunne e i propri alunni a valutare i rischi delle proprie frequentazioni virtuali.

Tra le misure di prevenzione che la scuola mette in atto ci sono, inoltre, azioni finalizzate a promuovere una cultura dell'inclusione, del rispetto dell'altro e delle differenze.
A tal proposito si è attivato uno "Sportello di ascolto" con lo scopo di raccogliere segnalazioni di casi di abuso, ponendo attenzione alle situazioni di disagio e avviare interventi a sostegno dello sviluppo della persona con personale specializzato.
Sono stati proiettati cortometraggi della campagna di comunicazione generazioni connesse ("I Super Errori), stimolo ed occasione per attivare dibattiti e riflessioni negli alunni.

Verranno posti negli spazi della scuola vicino le aule delle “Bull Box” nelle quali gli alunni possono inserire eventuali segnalazioni su casi di bullismo di cui sono stati vittime o spettatori.

4.2 I RISCHI E AZIONI DELLA SCUOLA

I rischi a cui sono esposti gli allievi sono numerosi, la Scuola quindi deve prenderli in considerazione tutti e pianificare azioni di prevenzione del rischio, rilevazione e gestione dei casi.

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, variando 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.
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*: affrontare 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 richiamarli 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:* affrontare 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. Chi è immerso dalla nascita nelle nuove tecnologie spesso non è consapevole che una foto o un video diffusi in rete potrebbero non essere tolti mai più né è consapevole di scambiare o diffondere materiale pedopornografico. In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico per gli adempimenti del caso.
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.

È fondamentale, perciò, far comprendere la nozione basilare secondo cui la propria ed altrui sicurezza in Rete non dipende solo dalla tecnologia adottata (software anti-virus, antimalware, apparati vari etc.) ma dalla capacità di discernimento delle singole persone nel proprio relazionarsi attraverso la Rete.

Azioni mirate alla sicurezza nella Rete sono, dunque, necessarie per affrontare tali problematiche: non vanno, infatti, colpevolizzati gli strumenti e le tecnologie e non va fatta opera repressiva di quest'ultime; occorre, viceversa, fare opera d'informazione, divulgazione e conoscenza per garantire comportamenti corretti in Rete, intesa quest'ultima come "ambiente di vita" che può dar forma ad esperienze cognitive, affettive e socio-relazionali. Da qui l'esigenza di definire linee di orientamento destinate al personale della scuola, agli studenti e alle famiglie che contengano indicazioni e riflessioni per la conoscenza e la prevenzione del

cyberbullismo e dei fenomeni ad esso riconducibili.

La Scuola inoltre si impegna su più fronti per ridurre i rischi di un uso non corretto delle TIC e della rete, contrastando il (cyber)bullismo in tutte le sue forme. A tale scopo ha programmato e realizzato le seguenti azioni:

- condividere materiali, aderire in ambito curriculare ad iniziative promosse dal MIUR e/o da altre Agenzie formative o da Enti pubblici e /o privati ed elaborare percorsi da proporre nelle classi per promuovere un uso consapevole delle TIC e di internet;
- proporre incontri specifici per studenti con funzionari che operano sul territorio per la tutela dei minori e il contrasto ai reati in rete (Polizia postale, Associazioni per la tutela dei minori);
- promuovere la diffusione della conoscenza delle Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo del MIUR.
- promuovere la partecipazione a percorsi di formazione finalizzati a sviluppare competenze informatiche nei docenti;

5. SEGNALAZIONE E GESTIONE DEI CASI

5.1 RILEVAZIONE

La rilevazione dei casi è a cura dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti. A partire dalla corretta formazione e sensibilizzazione, tutti gli adulti coinvolti, docenti e personale ATA sono invitati a essere confidenti e custodi, diretti o indiretti, di ciò che le ragazze e i ragazzi vivono: *si raccomanda di evitare ogni atteggiamento accusatorio o intimidatorio per riuscire a ricevere dai minori più fragili segnalazioni e confidenze circa situazioni problematiche vissute.*
Le/gli insegnanti in particolare sono chiamati a essere anche torre di avvistamento, spazio di avamposto privilegiato delle problematiche, dei rischi, dei pericoli che bambine, bambini e adolescenti possono vivere e affrontare ogni giorno. Accorgersi tempestivamente di quanto accade e compiere azioni immediate di contrasto verso gli atti inopportuni -quando non illegali diviene fondamentale per poter evitare conseguenze a lungo termine che possano pregiudicare il benessere e una crescita armonica dei soggetti coinvolti.

Intervenire in situazioni di Cyberbullismo non è mai semplice, spesso si pensa di non sapere cosa fare, temendo di essere inadeguati. La scuola quindi, ha individuato due strumenti utili ad agevolare l'intera comunità scolastica nel decidere come intervenire e nel tracciare i casi rilevati. Quest'ultima attività risulta estremamente importante al fine di un'adeguata revisione delle prassi da seguire per contrastare episodi che nel tempo potrebbero ripetersi.

5.2 SEGNALAZIONI

Uso improprio della rete

- accesso a siti inappropriati (pornografia, scommesse, giochi on-line non autorizzati dai docenti);
- accesso a credenziali personali;

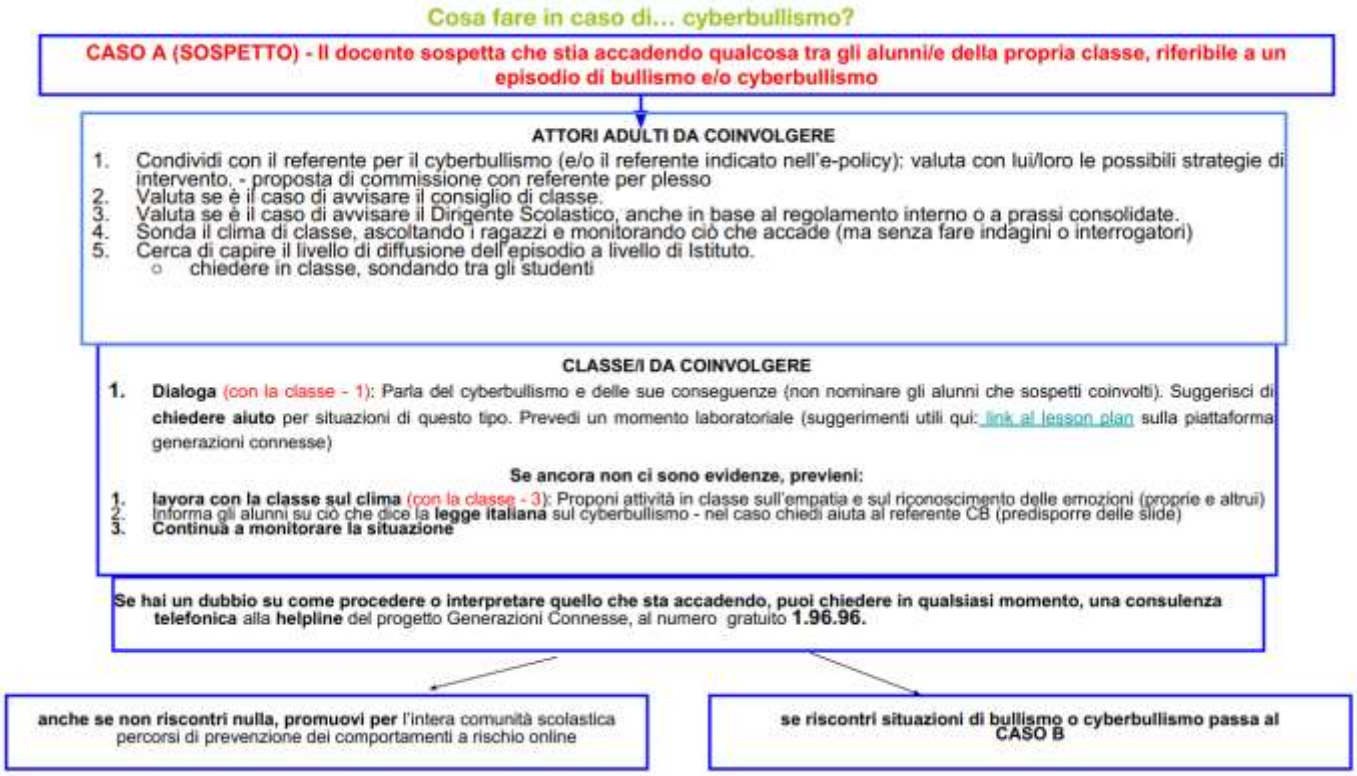
Cyberbullismo

Le tipologie di comportamenti online da segnalare sono:

- Offese e insulti tramite messaggi di testo, e-mail, pubblicati su social network o tramite telefono (ad esempio telefonate mute);
- Diffusione di foto o video che ritraggono situazioni intime, violente o spiacevoli tramite il cellulare, siti web o social network;

- Esclusione dalla comunicazione on-line, dai gruppi;
- Furto, appropriazione, uso e rivelazione ad altri di informazioni personali come le credenziali d'accesso all'account e-mail, social network, ecc.

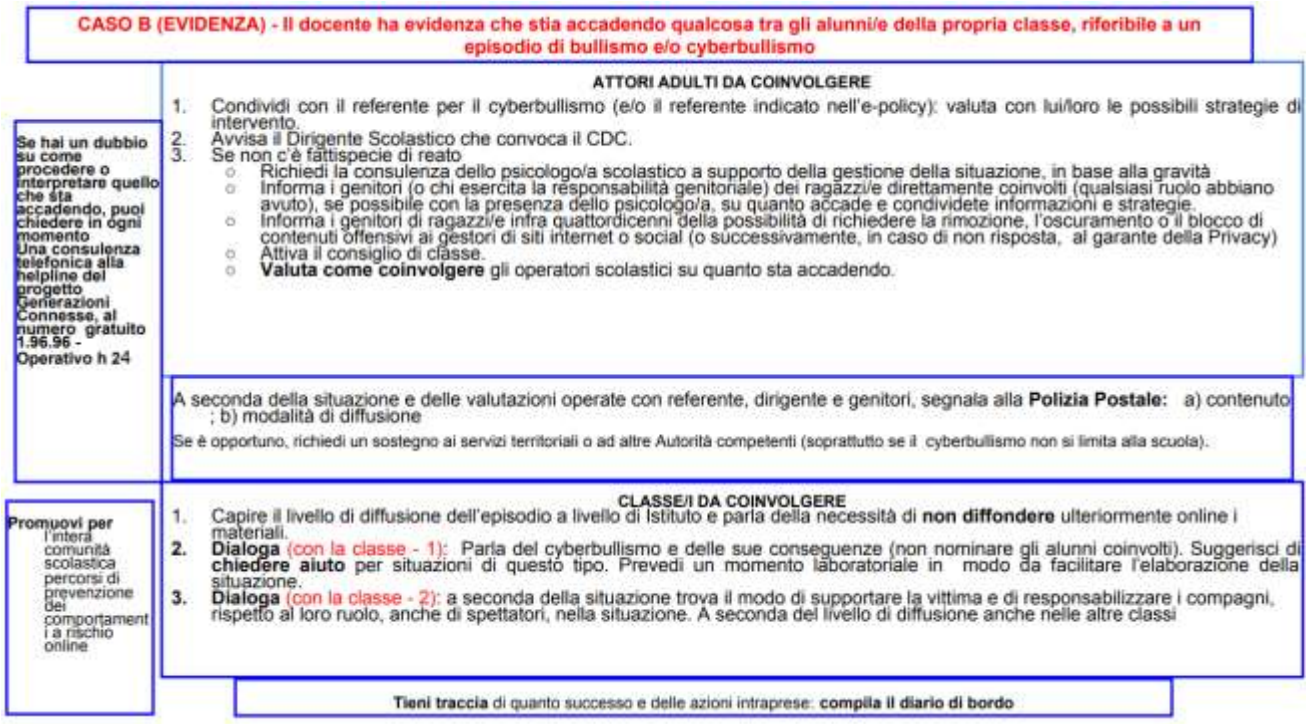
Accorgersi di episodi di (cyber)bullismo non è sempre facile perché le prevaricazioni avvengono in luoghi virtuali in cui gli adolescenti si ritrovano. Per cui è necessario cogliere i segnali che i ragazzi ci lanciano quando si trovano in una situazione di disagio o di difficoltà. Per interpretare meglio questi segnali seguirà lo schema d'intervento riportato di seguito:



Una "prova" di quanto riferito può essere presente nella memoria degli strumenti tecnologici utilizzati, può:

- essere mostrata spontaneamente dall'alunno;
- essere presentata da un reclamo dei genitori;
- essere notata dall'insegnante che si accorge dell'infrazione in corso.

Le tappe da seguire quando si presenta un caso di (cyber)bullismo sono riportate nello schema:



Gli strumenti per segnalare e monitorare i casi a scuola sono i seguenti:

- nell'effettuare la segnalazione seguire ed utilizzare il "modulo apposito di segnalazione" ALLEGATO 1 affinché le segnalazioni vengano effettuate per iscritto e contengano tutte le informazioni necessarie alla presa in carico della situazione.
- Utilizzare poi l'ALLEGATO 2 – "Diario di bordo" per tenere traccia di ciò che è avvenuto rispetto ai comportamenti dei tuoi alunni online e di come è stato gestito.

5.2.3 COME GESTIRE LE SEGNALAZIONI

La gestione dei casi rilevati va differenziata a seconda della loro gravità;

- fermo restando che è opportuna la condivisione a livello di Consiglio di Classe di ogni episodio rilevato, anche minimo, alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe.
- Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e come rimediare.
- Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico come intervenire.

Inoltre per i reati meno gravi la legge rimette ai genitori degli alunni la scelta di richiedere la punizione del colpevole, attraverso la querela. Per i reati più gravi (es. pedopornografia) gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti).
In particolare per i fatti criminosi, ai fini della denuncia, la relazione deve essere redatta ne modo più accurato possibile, indicando i seguenti elementi: il fatto, il giorno dell'acquisizione del fatto nonché le fonti di prova già note e per quanto possibile, le generalità, il domicilio e quant'altro di utile a identificare la persona alla quale il reato è attribuito, la persona offesa, e tutti coloro che sono in grado di riferire circostanze rilevanti per la ricostruzione del fatto.
Inoltre ci si potrà avvalere dei due servizi messi a disposizione dal Safer Internet Center: il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children.
Una volta ricevuta la segnalazione, infatti, gli operatori procederanno a coinvolgere le autorità competenti in materia.

In generale è bene tenere presente di:

- lavorare sul gruppo classe affinché riconosca la gravità dell'accaduto e la propria partecipazione attraverso il silenzio o forme blande di coinvolgimento;
- dare supporto al bullo con un programma educativo che si focalizzi su due fronti il coinvolgimento attivo del gruppo dei pari per sviluppare l'empatia e l'intervento dei docenti per gestire l'aggressività e la rabbia.

Come già detto per la prevenzione, il coinvolgimento dei coetanei è indispensabile per garantire l'efficacia dell'intervento ed è finalizzato a:

- creare un clima di solidarietà
- combattere l'indifferenza e la deresponsabilizzazione morale
- incoraggiare le vittime a chiedere aiuto
- sottrarre al (cyber)bullo potenziali proseliti

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.

Palermo, 08.02.2021

La Dirigente Scolastica
Prof.ssa Isabella Iervolino

L'Animatore Digitale
Prof.ssa Maria Karola Callea

Il referente per il bullismo e cyberbullismo
Prof.ssa Maria Pia Tantaro