UNIONE EUROPEA REPUBBLICA ITALIANA REGIONE SICILIANA

ISTITUTO COMPRENSIVO "SAURO-GIOVANNI XXIII"
e.mail ctic8a800e@istruzione.it- PEC ctic8a800e@pec.istruzione.it
Via T. Tasso, 2 – Tel. 095475037- Fax 095473442 - C.F. 93209870877
Cod. Mecc. CTIC8A800E
Sito web: WWW.ICSAURO-GIOVANNIXXIII.EDU.IT
95123 CATANIA

Capitolo 1 - Introduzione al documento di ePolicy

1.1 Scopo dell'Epolicy

L'Istituto Comprensivo "Sauro- Giovanni XXIII" di Catania ha elaborato il presente documento con lo scopo di informare l'utenza per un uso corretto e responsabile degli strumenti informatici collegati alla rete in dotazione alla scuola, nel rispetto della normativa vigente. Lo sviluppo delle Nuove tecnologie, nonché il loro utilizzo nella didattica e la grande diffusione nella vita di ognuno di noi di tali strumenti richiede una maggiore consapevolezza e responsabilità. Gli utenti, soprattutto minori, devono essere consapevoli dei rischi a cui si espongono quando navigano in rete. Gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, per prevenire il verificarsi di situazioni che possono rivelarsi pericolose.

1.2 Ruoli e responsabilità

Il Dirigente scolastico:

- garantisce la sicurezza on-line;
- garantisce la formazione del personale docente dell'uso delle TIC nella didattica;
- garantisce l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;
- segue le procedure previste dalle norme nel caso in cui ci siano reclami o attribuzione di responsabilità al personale scolastico in caso di incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.

L'Animatore digitale, supportato dal Team dell'innovazione:

- stimola la formazione interna alla scuola e negli ambiti di sviluppo della "scuola digitale";
- supporta il personale scolastico da un punto di vista tecnico;
- fornisce consulenza e informazioni relative ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- monitora e rileva le problematiche relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola;
- assicura che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate;
- coinvolge la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti alla "scuola digitale".

Il Referente del "Bullismo e del Cyberbullismo":

- coordina e promuove le attività specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo;
- si avvale della collaborazione di partner esterni alla scuola (servizi sociali e sanitari, forze di polizia, centri di aggregazione giovanile del territorio, ecc.) per realizzare un progetto di prevenzione con percorsi formativi che coinvolgano studenti, docenti e genitori.

Il Direttore dei servizi generali e amministrativi:

- assicura, 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;
- garantisce il funzionamento dei diversi canali di comunicazione all'interno della scuola e fra la scuola e le famiglie degli alunni tramite l'utilizzo del sito web della scuola.

I Docenti:

- diffondono la cultura dell'uso responsabile delle TIC e della rete;
- integrano parti del curriculum della propria disciplina con approfondimenti ad hoc;
- promuovono, dove è possibile, l'uso delle tecnologie digitali;
- garantiscono che gli alunni comprendano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di Internet;
- assicurano che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete, ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
- controllano l'uso delle tecnologie digitali da parte degli alunni durante le lezioni e ogni altra attività scolastica;

- guidano gli alunni a siti controllati e verificati come adatti per il loro uso nelle lezioni in cui è programmato l'utilizzo di Internet;
- controllano che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- segnalano al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di Internet, per l'adozione delle procedure previste dalle norme.

Gli Alunni:

- sono responsabili, in relazione al proprio grado di maturità e di apprendimento, nell'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- comprendono le potenzialità offerte dalle TIC per la ricerca di contenuti e materiali, evitando il plagio e rispettando i diritti d'autore;
- comprendono l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;
- adottano condotte rispettose degli altri anche quando si comunica in rete;
- sono promotori di quanto appreso con percorsi di peer education.

I Genitori:

- sono partecipi e attivi nella promozione ed educazione sull'uso consapevole delle TIC e della Rete;
- sono responsabili dell'uso dei device personali dei propri figli;
- seguono i figli nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti;
- si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete
- comunicano con i docenti circa i problemi rilevati quando i figli non usano responsabilmente le tecnologie digitali o Internet;
- accettano e condividono quanto scritto nell'e-policy dell'Istituto.

Il personale Amministrativo, Tecnico e Ausiliario (ATA):

- svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il Dirigente scolastico e con il Personale docente tutto.
- le suddette figure, in sinergia, si occupano ciascuno per la propria funzione, del funzionamento dell'Istituto scolastico attraverso lo sviluppo della cultura digitale e dell'organizzazione del tempo scuola.
- Il personale ATA è coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e

raccoglie, verifica e valuta le informazioni inerenti i possibili casi di bullismo/cyberbullismo.

1.3 Gli enti educativi esterni e le associazioni

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola, conformandosi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC, promuovono comportamenti sicuri -sicurezza online e protezione dei dati degli studenti e delle studentesse- durante le attività che si svolgono insieme.

1.4 Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

Il documento di ePolicy è condiviso con tutta la comunità scolastica, pone al centro gli studenti e le studentesse e sottolinea compiti, funzioni e attività reciproche.

Il testo sarà condiviso con:

studenti e studentesse

- per dare loro una base di partenza per un uso consapevole e maturo dei dispositivi e della tecnologia informatica;
- per dare loro regole condivise di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici;
- per dare loro elementi per poter riconoscere e quindi prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e.

il personale scolastico

- per poter orientare tutte le figure sui temi in oggetto, a partire da un uso corretto dei dispostivi e della Rete in linea anche con il codice di comportamento dei pubblici dipendenti;

i genitori che saranno informati attraverso il sito istituzionale della scuola, tramite momenti di formazione specifici e durante gli incontri scuola-famiglia.

1.5 Gestione delle infrazioni alla ePolicy

Prevenzione, rilevazione e gestione dei casi - Rischi

I rischi che possono insorgere a scuola nell'utilizzo delle TIC da parte degli alunni derivano dall'uso non corretto del telefono cellulare, dei tablet e dei pc della scuola collegati alla rete. Il telefono cellulare o lo smartphone non sono richiesti dalla scuola perché non sono ritenuti indispensabili in ambito scolastico, essi vengono forniti dai

genitori degli alunni per mantenere la comunicazione con i figli anche fuori dal contesto scolastico.

Disciplina degli alunni

Le infrazioni in cui gli alunni possono incorrere a scuola nell'utilizzo delle tecnologie digitali di Internet utilizzate per la didattica, sono prevedibilmente le seguenti:

- un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;
- la condivisione di dati personali come foto, l'indirizzo di casa o il numero di telefono;
- la condivisione di immagini intime e a sfondo sessuale;
- il collegamento a siti web non indicati dai docenti;
- l'invio di immagini o video con l'intento di escludere compagni/e.

E' necessario intervenire su tutto il contesto classe e i correttivi previsti sono rapportati all'età e al livello di sviluppo degli alunni.

Sono previsti da parte dei docenti provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento, quali:

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

Sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di prevenzione e gestione positiva dei conflitti, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni.

Disciplina del personale scolastico

Le possibili infrazioni in cui il personale scolastico può incorrere nell'utilizzo delle tecnologie digitali e di Internet sono di seguito elencate:

- una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- l'utilizzazione non 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.

Disciplina dei genitori

Condizioni e condotte dei genitori che possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola:

- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai;
- la posizione del computer nella stanza del proprio figlio, non visibile ai genitori;
- la piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone;
- un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei;
- un utilizzo del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria indirizzi o contenuti non idonei.

1.5 Integrazione dell'ePolicy con Regolamenti esistenti

Il presente documento si integra pienamente con il Regolamento Interno di Istituto e con il Patto di Corresponsabilità.

1.6 Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'aggiornamento della ePolicy sarà curato dal Team, dal referente del bullismo e cyberbullismo, dall'Animatore digitale con il coordinamento del Dirigente scolastico. Avrà il fine di rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di Internet.

Capitolo 2 - Formazione e curricolo

2.1 Curricolo sulle competenze digitali per gli studenti

I ragazzi utilizzano il web in modo quotidiano mostrando a volte particolari doti di immediatezza e versatilità nel padroneggiare le applicazioni e la navigazione sui dispositivi mobili personali, ma non per questo sono dotati di maggiori "competenze digitali" rispetto agli adulti. Infatti per competenza digitale si intende la passione e l'interesse per le tecnologie digitali e il loro utilizzo con spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Questa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e

possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico" ("Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente", C189/9, p.9).

Proprio a tal fine, il nostro Istituto si impegna a portare avanti percorsi volti a promuovere tali competenze, con la finalità di educare gli studenti ad un uso consapevole e responsabile delle tecnologie digitali. Questo però è reso possibile tramite una mirata progettazione ed implementazione di un curricolo digitale.

L'Agenda 2030 ha messo in evidenza come lo sviluppo sostenibile, declinato in vari obiettivi, verrà promosso e favorito dalla competenza digitale e dalle meta-competenze, come l'empatia, la resilienza, la creatività, il pensiero critico. L'Educazione, pertanto, gioca un ruolo chiave nel nuovo scenario culturale che si sta delineando, non solo perché le competenze richieste per l'inserimento nel mondo del lavoro sono in continua evoluzione, ma anche perché, proprio grazie alle tecnologie, cambia il modo di trasferire e declinare queste "skills". Diventa perciò necessario per l'apprendimento costruire un curriculo verticale che porti ogni alunno a sviluppare competenze digitali che gli consentiranno gradualmente una cittadinanza sempre più consapevole, inclusiva, responsabile, attiva e partecipe. L'I.C. "Sauro – Giovanni XXIII" di Catania si è dotato già negli ultimi anni di un curricolo per competenze in cui è contemplata la competenza digitale, ritenuta dall'Unione Europea competenza chiave, trasversale alle discipline previste dalle Indicazioni Nazionali per la sua importanza e diffusione nel mondo d'oggi. Possedere una competenza digitale significa padroneggiare certamente le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con "autonomia e responsabilità", con spirito critico, nel rispetto degli altri e sapendone prevenire ed evitare i pericoli. In questo senso, tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione. Pertanto, per sostenere questo processo, all'interno della scuola è necessario investire sulla formazione e sull'aggiornamento degli insegnanti, soprattutto in relazione alla didattica per competenze con particolare attenzione a quella digitale. Alcune classi dell'Istituto hanno inoltre aderito già a partire dall'a.s. 2016/2017 al progetto ministeriale "Programma il futuro" coinvolgendo gli alunni nella sperimentazione del coding (Code Week e l'ora del coding), integrando così le competenze digitali già previste dalle Indicazioni Nazionali, attraverso la promozione dello sviluppo del "pensiero computazionale" negli alunni. Attività di sensibilizzazione sull'uso corretto delle tecnologie digitali con iniziative hanno visto il coinvolgimento degli alunni di tutte le classi in occasione nella giornata del *Safer Internet Day* per la Scuola Secondaria di I grado. Sono state anche proiettate in auditorium diversi film e documentari sulle tematiche inerenti al bullismo ed al cyberbullismo rivolti agli studenti della Scuola Secondaria di I grado e alle classi quinte della Scuola Primaria.

Sono stati, a tal proposito, realizzati degli incontri informativi e di sensibilizzazione con la referente al bullismo e cyberbullismo e con la Polizia Postale.

2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

Ciò si rende necessario per fornire agli studenti modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

La competenza digitale, oggi, è imprescindibile per i docenti così come per tutti gli studenti del nostro Istituto e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa e in grado di venire incontro ai nuovi stili di apprendimento.

Il nostro Istituto, come si evince dal RAV e dal PDM, promuove lo sviluppo delle competenze digitali degli studenti, con particolare riguardo al pensiero computazionale, all'utilizzo critico e consapevole dei social network e dei media nonché alla produzione e ai legami con il mondo del lavoro. Promuove l'uso delle TIC nella didattica e la formazione digitale continua del personale docente.

La formazione interna alla scuola sui temi del PNSD è organizzata dall'Animatore Digitale, col supporto del Team digitale, al fine di favorire la partecipazione e stimolare il protagonismo degli studenti nell'organizzazione di workshop e altre attività, anche aprendo i momenti formativi alle famiglie e ad altri attori del territorio, per la realizzazione di una cultura digitale condivisa.

Già da qualche anno, la scuola attua per gli alunni della Scuola Secondaria di I Grado il Progetto "Edu Robot". E' un progetto che coinvolge gli studenti stimolando il pensiero computazionale e il problem solving.

La scuola attua già dall'anno scorso la didattica digitale integrata tramite l'uso di applicazioni svolte in modalità sincrona e asincrona, soprattutto con l'ausilio della piattaforma GSuite e in qualche classe anche tramite altre piattaforme (Padlet ed Edmodo). Inoltre, la scuola ha ottenuto diversi finanziamenti attraverso i progetti PON/FSEPON SI per l'acquisto di pc e software per la didattica digitale.

Entro il prossimo triennio intende partecipare a progetti di partneriato e-Twinning promossi da Erasmus Plus.

La formazione esterna prevede la partecipazione dei docenti ai progetti realizzati dalle scuole in relazione all'adesione alla rete come è già avvenuto negli anni scorsi con la formazione in rete promossa dall'ambito 10 della provincia di Catania.

Inoltre, è prevista la partecipazione a seminari, convegni, corsi on-line organizzati dagli Enti del territorio, dalle scuole in rete che partecipano al PNSD, da esperti interni alla scuola che rientreranno nell'organico di potenziamento e da esperti esterni a pagamento;

tali interventi saranno rivolti:

· ai docenti;

· al personale amministrativo;

· ai collaboratori scolastici;

· alle famiglie, destinatarie di servizi on-line;

Il processo avverrà in modo graduale e riguarderà gli anni scolastici dal 2020 al 2023.

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

L'Istituto Comprensivo "Sauro – Giovanni XXIII" di Catania si avvale della figura dell'Animatore digitale che, con il Dirigente Scolastico e il D.S.G.A., collabora per raggiungere gli obiettivi di innovazione del PNSD nella scuola. Inoltre, a partire dall'anno scolastico 2017-2018 è attiva la figura del Referente d'Istituto per le attività di prevenzione e contrasto al bullismo e al cyberbullismo (L.71/2017). La formazione sull'utilizzo consapevole e sicuro delle TIC è stata estesa ad altre figure, in funzione della costituzione di un Team per le emergenze. Si rende, comunque, necessaria la formazione di tutti i docenti sull'uso consapevole e sicuro di Internet e sui rischi della rete. Infatti il percorso di formazione specifica dei docenti dovrebbe essere permanente in relazione all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono in maniera costante ed autonoma i ragazzi. La formazione potrà prevedere momenti di autoaggiornamento e di formazione personale o collettiva, anche attraverso corsi dedicati, seminari, conferenze, dibattiti webinar ecc.

2.4 Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Scuola e famiglia sono chiamate a collaborare per garantire la crescita formativa di ciascun alunno, perciò stipulano all'inizio dell'anno scolastico il Patto Educativo di Corresponsabilità. Alla luce del progresso e dell'evoluzione delle tecnologie, l'Istituto attiverà iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine saranno previsti incontri fra docenti e/o esperti e genitori sui temi

oggetto della Policy per la diffusione del materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati (Generazioni Connesse) e dalle forze dell'ordine. Sul sito della scuola, inoltre, sarà pubblicato il presente documento per la divulgazione delle informazioni e delle procedure contenute, per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'Istituto e per prevenire i rischi legati ad un utilizzo scorretto di Internet.

Con riferimento a quanto previsto dalla legge 29.5.2017, n.71 e all'aggiornamento delle Linee di orientamento per la prevenzione e il contrasto del cyberbullismo (nota MIUR prot. n. 5515 del 27-10-2017), alla famiglia spetta l'obbligo/l'impegno a vigilare e educare i propri figli con riferimento alla prevenzione dei fenomeni di bullismo e cyberbullismo ed alla Scuola l'impegno a prevenire e a contrastare il bullismo e il cyberbullismo promuovendo la conoscenza e la diffusione delle regole relative al rispetto tra gli studenti, alla tutela della loro salute, alla corretta comunicazione e al corretto comportamento sul web. Si rende pertanto necessario integrare il Patto di Corresponsabilità di Istituto con riferimenti specifici all'uso delle tecnologie digitali e all'ePolicy al fine di portare le famiglie a conoscenza del piano d'azione previsto comprensivo di:

- regole sull'uso delle tecnologie digitali da parte dei genitori nelle comunicazioni con la scuola e con i docenti (es. mail, gruppo WhatsApp, sito della scuola, registro elettronico etc.) e anche riguardo alle regole per gli studenti;
- consigli o linee guida sull'uso delle tecnologie digitali nella comunicazione con i figli e in generale in famiglia;
- percorsi di sensibilizzazione e formazione dei genitori e degli studenti su un uso responsabile e costruttivo della Rete in famiglia e a scuola.

Il nostro piano d'azioni:

AZIONI da sviluppare nell'arco del triennio 2020/2021, 2021/2022, 2022/202.)

L'Istituto prevede di sviluppare a partire dall'anno scolastico 2020/2021 le seguenti

Azioni:

- effettuare un'analisi del fabbisogno formativo su un campione di studenti in relazione alle competenze digitali.
- effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

- coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.

Nell'arco del triennio saranno sviluppate le seguenti azioni:

- promuovere per il corpo docente incontri formativi/webinar sull'utilizzo e l'integrazione delle TIC nella didattica.
- promuovere per il corpo docente incontri/webinar formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- promuovere incontri/webinar con esperti per i docenti sulle competenze digitali.
- promuovere incontri/webinar con esperti per i genitori sull'educazione alla cittadinanza digitale.

Capitolo 3 - Gestione dell'infrastruttura e della strumentazione ICT della e nella scuola

3.1 Protezione dei dati personali

In merito alla protezione dei dati personali, si fa riferimento a quanto previsto dal Decreto Legislativo del 30 giugno 2003, n.196 (cosiddetto Codice della Privacy), integrato dal D. Lgs. 10 agosto 2018, n. 101, e dal GDPR (General Data Protection Regulation) n. 679 del 2016. All'atto dell'iscrizione viene fornita ai genitori informativa e richiesta di autorizzazione sull'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori, come ad esempio l'utilizzo di fotografie, video o altri materiali audiovisivi contenenti l'immagine e/o il nome del proprio figlio/a all'interno di attività educative e didattiche per scopi documentativi, formativi e informativi, durante gli anni di frequenza della scuola. A tale proposito, si evidenzia che le immagini e le riprese audiovideo realizzate dalla scuola, nonché gli elaborati prodotti dagli studenti durante le attività scolastiche, potranno essere utilizzati esclusivamente per documentare e divulgare le attività della scuola tramite il sito Internet di Istituto. L'autorizzazione non consente l'uso dell'immagine in contesti che pregiudichino la propria dignità personale ed il decoro e comunque per uso e/o fini diversi da quelli sopra indicati. Inoltre, in caso di partecipazioni a concorsi o manifestazioni l'Istituto richiede apposita autorizzazione, chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato all'interno di modulistica o sul proprio sito web istituzionale. La formula utilizzata per chiedere il consenso è, in ogni caso, comprensibile, semplice e chiara. Pertanto, in ottemperanza al GDPR (General Data Protection Regulation) e al D. Lgs. 10 agosto 2018, n. 101, entrato in vigore lo scorso 19 settembre, la scuola non si impegna solo a tutelare la privacy degli/lle studenti/esse e delle loro famiglie, ma anche ad informare e soprattutto

rendere consapevoli gli/le studenti/esse di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri.

3.2 Accesso ad Internet

L'accesso a Internet è possibile e consentito per la didattica in tutti i plessi della primaria e della secondaria di primo grado attraverso reti WiFi. La Dirigenza e l'Amministrazione hanno una rete separata. Il docente segnala alla Dirigenza eventuali malfunzionamenti e disservizi della strumentazione a disposizione. E' attivo un filtro di protezione per la navigazione dei minori sui computer utilizzati dagli alunni per l'accesso ad Internet. L'accesso a Internet, attraverso i dispositivi della scuola da parte degli studenti, avviene solo in presenza dell'insegnante, il quale è responsabile del comportamento degli alunni, delle macchine e del software che utilizzano. È possibile effettuare installazioni e aggiornamenti di software solo tramite la password di amministratore, fornita al personale di assistenza tecnica. L'accesso al sistema informatico per la didattica è consentito al personale attraverso l'assegnazione di una password. L'accesso ai portali istituzionali come SIDI, Istanze on-line, alla Segreteria Digitale, PON ecc. prevede l'uso di credenziali personali, mentre l'accesso a portali tematici si effettua per mezzo di password uniche condivise tra i referenti di progetti e/o azioni e la Dirigenza. I docenti possono accedere alla propria sezione del registro elettronico con credenziali personali. I computer presenti nelle aule non richiedono una password di accesso per l'accensione. L'account di posta elettronica è quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. Anche tutti i docenti dell'Istituto e gli studenti iscritti possiedono un account generato dalla scuola per consentire loro l'accesso alla piattaforma didattica per la DAD. L'Istituto attualmente, grazie alla partecipazione ai bandi PON, in classi della Primaria e dell'Infanzia, è dotato di una rete wireless destinata all'utilizzo didattico da parte del corpo docente e degli alunni che utilizzano le LIM nella Scuola dell'Infanzia e nella Scuola Primaria e i tablet in dotazione dell'Atelier Creativo nella Scuola Secondaria di I grado. La password viene fornita dall'amministratore della rete o dall'Animatore Digitale. Ogni accesso viene registrato con credenziali rilasciate in modalità permanente o guest. Ciascun utente connesso alla rete dovrà: rispettare il presente regolamento e la legislazione vigente succitata, tutelare la propria privacy, quella degli altri utenti adulti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui ha accesso.

Al fine di garantire la safety nell'accesso ad Internet gli studenti saranno guidati allo sviluppo di competenze digitali per un uso consapevole delle TIC e della RETE e al rispetto della "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).

La security sarà invece implementata attraverso l'adozione delle seguenti misure cautelative:

- mantenere separate le reti didattica e segreteria -importante per garantire maggiore sicurezza alle informazioni, gestendo in modo autonomo e con regole differenti le due reti grazie al firewall;
- aggiornare periodicamente software e Sistema operativo -garantire che il sistema sia aggiornato lo protegge dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo.
- definire la programmazione di backup periodici, cioè la copia e messa in sicurezza dei dati del sistema scolastico per prevenire la perdita degli stessi (possibilmente anche una copia offline);
- garantire formazione adeguata allo staff, incluso il corpo docente -la formazione deve riguardare la gestione dei dispositivi, la conoscenza delle regole basilari sulla sicurezza.
- preparare piani di azione in risposta ai problemi più seri -è importante non dover improvvisare nel momento in cui si verifica un problema serio, ma avere un protocollo di azione.
- predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo -se non è previsto uno stand-by, il dispositivo resta accessibile nel caso in cui qualcuno dimentichi di spegnerlo, con il rischio potenziale di accesso da parte di persone non autorizzate.
- impostare il browser per l'eliminazione dei cookies alla chiusura -in questo modo si evita che qualcuno possa avere accesso ad account altrui senza autorizzazione.
- definire una policy sulle password.
- sviluppare il regolamento sull'uso delle tecnologie a scuola (policy di uso accettabile): deve riguardare chiunque abbia accesso alla Rete, studenti/esse, docenti, amministrazione e segreteria, includere i dispositivi della scuola e quelli personali, anche in caso di BYOD.

3.3 Strumenti di comunicazione online

Il sito dell'Istituto Comprensivo è raggiungibile all'indirizzo https://icsauro-giovannixxiiii.edu.it. La gestione del sito della scuola e la rispondenza alle normative per quanto concerne i contenuti (accuratezza, appropriatezza, aggiornamento) e le tecniche di realizzazione e progettazione è a cura del Dirigente Scolastico e del webmaster responsabile del sito. Sul sito è possibile trovare il Regolamento d'Istituto,

pubblicizzazione di eventi, avvisi ai genitori, documentazione di attività curricolari ed extracurricolari svolte. È possibile accedere all'area riservata del sito dove sono caricate le comunicazioni interne. L'accesso a tale area non è nominativo, ma è stata creata un'unica credenziale per tutti. La scuola, in qualità di ente pubblico, pubblicherà sul proprio sito web i contenuti che saranno valutati come pertinenti alle finalità educative istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative.

3.4 Strumentazione personale

I docenti utilizzano i telefoni cellulari durante l'orario di lavoro solo per le attività didattiche. L'I.C. "Sauro-Giovanni XXIII" dispone il divieto dell'utilizzo del cellulare o di altri dispositivi elettronici per uso personale da parte degli alunni. È consentito il loro utilizzo previa autorizzazione del docente e sempre se finalizzato ad un uso strettamente didattico. La violazione di tale divieto configura un'infrazione disciplinare rispetto alla quale la scuola è tenuta ad applicare apposite sanzioni. E' consentito l'uso di dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili.

Per implementare la dotazione scolastica relativa alle TIC e favorire il BYOD il nostro Istituto si impegna a fornire delle credenziali a tempo per gli alunni che ne facciano richiesta (alunni DSA, BES e diversamente abili in primis).

Il nostro piano d'azioni

AZIONI (da sviluppare a partire dall'anno scolastico 2020/2021).

- effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti.
- effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti.
- effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA.
- organizzare eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola.

AZIONI (da sviluppare nell'arco dei tre anni 2020/2022).

- promuovere incontri per la consultazione degli studenti su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- promuovere incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali

- promuovere eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali (in collaborazione con il GPDR)
- promuovere eventi o attività volti a formare gli studenti dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- promuovere eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- promuovere eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie
- promuovere eventi o attività volti a formare gli studenti dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (anche in concomitanza del "*Safer Internet Day*").

Capitolo 4 - Rischi on line: conoscere, prevenire e rilevare

4.1 Sensibilizzazione e Prevenzione

Il rischio in cui gli studenti possono incorrere, con l'utilizzo della rete, fa sì che la scuola metta in atto un processo di sensibilizzazione all'utilizzo delle tecnologie digitali in rete.

L'Istituto Comprensivo "Sauro/Giovanni XXIII" di Catania intende perseguire azioni di prevenzione universale e di sensibilizzazione, con l'autorizzazione delle famiglie e la collaborazione della rete di servizi territoriali locali (Polizia Postale, ASP, Servizi Sociali ecc...), atti a formare e consolidare competenze educative necessarie a poter gestire e arginare i rischi derivanti dalla navigazione in rete.

Gli strumenti necessari per poter ridurre e contrastare tali rischi sono gli interventi di sensibilizzazione e prevenzione.

Sensibilizzazione attraverso azioni utili a far conoscere il fenomeno anche attraverso illustrazioni, comportamenti da adottare e possibili soluzioni.

Prevenire attraverso attività, azioni, interventi atti a promuovere competenze digitali tali da far riconoscere ed evitare l'insorgenza dei rischi legati alla rete.

4.2 Cyberbullismo; che cos'è e come prevenirlo

Il Cyberbullismo è la manifestazione in rete del fenomeno del bullismo perpetrato in rete attraverso i social network, con la diffusione di messaggi offensivi, foto e immagini denigratorie o tramite la formazione di gruppi contro una presunta vittima.

Il nostro ordinamento giuridico fino a poco tempo fa non contemplava una definizione di Cyberbullismo, ma con la legge del 29 Maggio del 2017 n. 71 riguardante le "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del Cyberbullismo". Nell'articolo 1 comma 2 con il termine Cyberbullismo si intende qualunque forma di pressione, aggressione, molestia, ricatto, denigrazione, diffamazione, furto di identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali a danno dei minorenni, realizzata per via telematica, nonchè la diffusione dei contenuti on-line aventi ad oggetto anche uno o più componenti della famiglia del minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso o la loro messa in ridicolo.

La stessa legge e le relative Linee di orientamento per la prevenzione e il contrasto del cyberbullismo indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

- Formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- Sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- Promozione di un ruolo attivo degli studenti in attività di peer education; previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;

Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.

La scuola individua i Referenti per le iniziative di prevenzione e contrasto che avranno il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di Polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.

Le azioni messe in atto dall'Istituto sono:

- coinvolgere genitori, studenti, e tutto il personale scolastico in progetti sull'educazione alla legalità e all'uso consapevole di internet;
- coordinare incontri fra i docenti e stabilire regole condivise per la prevenzione dei fenomeni di Bullismo e Cyberbullismo;
- prevedere azioni culturali con gli studenti per acquisire le competenze necessarie all'esercizio di una cittadinanza digitale consapevole.

All'inizio dell'anno scolastico, i docenti presenteranno alle famiglie il documento prodotto che racchiude regole e azioni per affrontare il fenomeno del Bullismo e del

Cyberbullismo, un insieme di norme comportamentali e attività per favorire lo sviluppo di una cittadinanza attiva e responsabile nell'utilizzo delle TIC in ambiente scolastico e non.

Ogni docente svolgerà attività di prevenzione del fenomeno:

- dedicando alcune lezioni sull'utilizzo consapevole di internet;
- migliorando l'approccio socio relazionale all'interno delle classi;
- proponendo la visione di cortometraggi e film, stimolo ed occasione per attivare dibattiti e riflessioni negli alunni;
- partecipazione al Safer Internet Day.

A seconda dei casi, si potranno adottare azioni di prevenzione universale, selettiva e indicata.

1**. Prevenzione Universale**. Un programma di questo tipo parte dal presupposto che tutti gli studenti siano potenzialmente a rischio. Si tratta quindi di interventi diretti al grande pubblico o a un intero gruppo di una popolazione che non è stato identificato sulla base del rischio individuale. Efficacia: trattandosi di programmi ad ampio raggio gli effetti di questi programmi possono essere modesti se confrontati con programmi che "trattano" un gruppo con un problema specifico. Tuttavia, questi interventi possono produrre cambiamenti in grandi popolazioni (ad es. si pensi ad un programma dedicato alle competenze emotive, oppure alla cittadinanza digitale).

2**. Prevenzione Selettiva**. Un programma dedicato ad un gruppo di studenti in cui il rischio online è presente. In questo caso la presenza del rischio è stata individuata tramite precedenti indagini, segnalazioni fatte dalla scuola, oppure dalla conoscenza della presenza di fattori di rischio in quel determinato territorio. In questi casi gli interventi sono mirati e prevedono programmi formativi strutturati che hanno l'obiettivo di migliorare le competenze digitali e le strategie di problem solving. Può essere un valido programma se si osservano casi in cui la prevenzione universale non ha dato gli esiti previsti.

3**. Prevenzione Indicata**. Un programma di intervento sul caso specifico, è quindi pensato e strutturato per adattarsi agli/lle studenti/studentesse con l'obiettivo di ridurre i comportamenti problematici, oppure dare supporto alle vittime. Per la sua natura questo tipo di intervento si avvale di professionalità diverse perché spesso affronta problemi legati alla salute mentale del minore per cui è opportuno coinvolgere anche la famiglia del/lla ragazzo/a.

4.3 Le tipologie di cyberbullismo maggiormente considerate

- Hate speech. Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo on-line) che esprimono

odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena.

Più ampiamente il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo. Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono quindi un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete. Occorre, in tal senso, valorizzare la dimensione relazionale e fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità; promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network; favorire una presa di parola consapevole e costruttiva da parte dei giovani. Inoltre, l'Istituto si potrà avvalere di consulenti/esperti per organizzare incontri formativi rivolti a docenti, genitori ed alunni (Carabinieri, Polizia Postale, equipe Formazione Territoriale del MIUR, associazioni del Territorio preposte allo scopo...).

L'Istituto si propone di promuovere un uso maggiormente consapevole delle tecnologie e mantenere una relazione sana.

Gli elementi che contribuiscono al benessere digitale sono:

- la ricerca di equilibrio nelle relazioni anche on-line,
- l'uso degli strumenti digitali per il raggiungimento di obiettivi personali,
- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile,
- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche).

È importante non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli studenti e delle studentesse, strutturando chiare e semplici regole condivise. Inoltre, sarà fondamentale concordare una linea condivisa con la famiglia, per stabilire mezzi e modalità durante lo studio domestico, con forme di controllo attivo durante la navigazione in Rete.

- **Dipendenza da internet e dal gioco online** (i comportamenti patologici/dipendenze). La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete. Tale dipendenza, che può manifestarsi anche attraverso le ore trascorse on-line a giocare, rappresenta una questione importante per la comunità scolastica, che deve rilevare il fenomeno e fornire gli strumenti agli studenti e alle studentesse affinché questi siano consapevoli dei rischi che comporta l'iperconnessione.

L'Istituto si propone di promuovere un uso maggiormente consapevole delle tecnologie, per favorire il "benessere digitale", ossia la capacità di instaurare e mantenere una relazione sana con la tecnologia.

Gli elementi che contribuiscono al benessere digitale sono:

- la ricerca di equilibrio nelle relazioni anche on-line,
- l'uso degli strumenti digitali per il raggiungimento di obiettivi personali,
- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile,
- la capacità di gestire il sovraccarico informativo e le distrazioni.

È importante non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli studenti e delle studentesse, strutturando chiare e semplici regole condivise. Inoltre, sarà fondamentale concordare una linea condivisa con la famiglia, per stabilire mezzi e modalità durante lo studio domestico, con forme di controllo attivo durante la navigazione in Rete.

- **Sexting** (scambio di contenuti mediali sessualmente espliciti). Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti mediali sessualmente espliciti. I ragazzi lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video. Spesso tali immagini o video, anche se inviate ad una stretta cerchia di persone, si diffondono in modo incontrollabile, perché facilmente modificabili, scaricabili e condivisibili e possono creare seri problemi, sia personali che legali, alla persona ritratta. L'invio di foto che riguardano minorenni in pose sessualmente esplicite configura, infatti, il reato di distribuzione di materiale pedopornografico.

I rischi del sexting, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro e depressione.

- **Il grooming o adescamento online** (una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata). Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro. I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di teen dating (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online. La problematica dell'adescamento online (come quella del sexting) si inquadra in uno scenario più ampio di scarsa educazione emotiva, sessuale e di assenza di competenza digitale. Al fine di prevenire casi di adescamento online è opportuno, pertanto, accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità.

È importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Fondamentale quindi, è portare avanti un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni on-line (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è). Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere, ad esempio, all'adescatore. È importante che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove. Casi di adescamento on-line richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video…). L'adescamento, inoltre, può essere una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore.

- **Denigration** (diffusione di pettegolezzi, insulti, voci lesivi della dignità della persona).

- **Body shaming** (prendere in giro per l'aspetto fisico).

- **Pedopornografia.** La pedopornografia on-line è un reato che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video

ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, concrete o simulate o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali. In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere. La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting. Qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione "Segnala contenuti illegali" (Hotline).

Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia. L'intento è quello di facilitare il processo di rimozione del materiale stesso dalla Rete e allo stesso tempo consentire le opportune attività investigative finalizzate ad identificare chi possiede quel materiale, chi lo diffonde e chi lo produce, ma, soprattutto e primariamente, ad identificare i minori abusati presenti nelle immagini e video, assicurando la fine di un abuso che potrebbe essere ancora in corso e il supporto necessario. Parallelamente, per salvaguardare il benessere psicofisico degli alunni coinvolti nella visione di questi contenuti, sarà opportuno ricorrere a un supporto psicologico anche passando per una consultazione presso il medico di base o pediatra di riferimento.

Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza: Consultori Familiari, Servizi di Neuropsichiatria infantile, centri specializzati sull'abuso e il maltrattamento all'infanzia, etc. Se si è a conoscenza di tale tipologia di reato è possibile far riferimento alla: Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Polizia di Stato – Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato – Commissariato online.

Capitolo 5 - Segnalazione e gestione dei casi

Al fine di aiutare gli studenti e le studentesse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, si prevedono strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserita in uno spazio accessibile e ben visibile della scuola, al piano della segreteria sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

Sono considerati casi da segnalare:

- contenuti afferenti la violazione della privacy (foto personali, indirizzo o numero di telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà ecc..)
- contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi pettegolezzi informazioni false, foto o video imbarazzanti e umilianti, virus, contenuti razzisti che inneggiano al suicidio, insulti ecc..)
- contenuti afferenti alla sessualità: messaggi molesti, conversazioni che connotano una relazione intima e/o sessualizzata, foto e video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e/o video in cui minori sono coinvolti o assistono ad attività sessuali (pedopornografia).

5.2 Come segnalare: quali strumenti e a chi?

Per quanto riguarda la gestione dei casi, il nostro Istituto ha individuato una figura referente per il cyberbullismo.

La segnalazione del caso dovrà quindi essere fatta dal singolo docente, tramite modulo allegato al presente documento (Allegato 2), alla referente, la quale, insieme al Team per le emergenze, si occuperà di raccogliere tutte le informazioni possibili, anche attraverso colloqui di approfondimento con gli attori coinvolti e di segnalare l'accaduto al Dirigente.

Il Dirigente, insieme al Team, valuterà se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali o se il caso vada gestito all'interno della scuola con il coinvolgimento del Consiglio di Classe e delle famiglie degli alunni coinvolti.

Si sceglierà uno o più interventi da attuare a cui seguirà una fase di monitoraggio.

Deliberato dal Collegio dei Docenti nella seduta del 26/11/2020.

Il Dirigente Scolastico
Prof.ssa Francesca Condorelli
documento firmato digitalmente

Allegato 1

MODULO SEGNALAZIONE ATTI BULLISMO/CYBERBULLISMO A SCUOLA

AL DIRIGENTE SCOLASTICO
dell' I.C. Sauro-Giovanni XXIII
Catania
e p.c. al Referente al cyberbullismo

COMPILATORI: [ ] docente [ ] genitore [ ] alunno della classe ……

- Nome e Cognome

……

- Indicare sede e/o plesso in cui è avvenuto l'episodio

……

……

- Chi è l'alunno che ha subito atti di bullismo e/o cyberbullismo?

Nome e cognome…….classe……..sezione……..

Quando?.....

- In quale ambiente della scuola?

Cortile esterno O aula O bagni O corridoi O palestra O aula informatica O

Laboratorio scientifico O altro O ……

- Come si chiama l'autore del presunto atto di bullismo e/o cyberbullismo?

……

- Quale classe frequenta?

……

- Ha agito da solo? Sì No

- Se no come si chiamano e che classe frequentano i compagni che lo affiancavano?

…….

- Chi ha assistito all'episodio?

…….

- E' la prima volta che accade? Sì No

- Se no da quanto tempo accade questo episodio?

…….

- La vittima è stata minacciata di non raccontare il fatto? Sì No - Se sì da chi?

…….

- Con quali modalità si sono svolti i fatti? (Descrivere l'accaduto?)

……

……

…….

Catania, _____/_____/_____ _____

Firma

[ ] docente [ ] genitore [ ] alunno che effettua la segnalazione

Allegato 2

PROCEDURA PER CASO DI PRESUNTO BULLISMO E VITTIMIZZAZIONE A SCUOLA

1. Prima segnalazione
2. Valutazione approfondita
3. Gestione del caso attraverso uno o più interventi:
    - Approccio educativo con la classe
    - Intervento individuale
    - Gestione della relazione
    - Coinvolgimento della famiglia
    - Supporto intensivo a lungo termine e di rete
4. Monitoraggio