MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITA' E DELLA RICERCA
UFFICIO SCOLASTICO REGIONALE DELLA CAMPANIA
DIREZIONE DIDATTICA STATALE SCAFATI I
Via S. Antonio Abate 84018 - SCAFATI - Telefono e Fax 0818631737
e-mail: saee16100t@istruzione.it;
pec: saee16100t@pec.istruzione.it; sito web: http://www.1circoloscafati.edu.it
C.M. SAEE16100T - C.F. 80033520653

Documento di e-Policy

A.S. 2020/2021

Istituto : D.D.S. Scafati I

team ePolicy:

Dirigente dott.ssa Maria d'Esposito
Ins.Annunziata Manfredini
Ins.Eleonora di Martino
dott.ssa Concetta Arnone
Ins.Rosanna Falanga

VISTA la LEGGE n. 71/2017 sulla "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" ed in particolare l'Art. 5.2. I regolamenti delle istituzioni scolastiche di cui all'articolo 4, comma 1, del regolamento di cui al decreto del Presidente della Repubblica 24 giugno 1998, n. 249, e successive modificazioni;

VISTE ie "Linee di Orientomento per lo prevenzione e il controsto del bullismo e cyberbullismo"del 2021, in continuita con ie precedenti "Linee di Orientomento per lo prevenzione e il controsto del cyberbullismo"del 7OT7 e 2015;

VISTO il Piano Triennale dell'0fferta Formativa, in cui viene dato rilevanza a

VISTO il Patto di Corresponsabilita (D.P.R. 23) ed in particolare il riferimento a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alia gravita degli atti compiuti .

VISTO il Regolamento di Istituto ed in particolare il riferimento a condotte di bullismo e di cyberbullismo e relative sanzioni disciplinari commisurate alia gravita degli atti compiuti,

DICHIARAZIONE DI INTENTI

L'Istituto Scolastico *DDS I circolo di Scafati* si impegna a garantire alia propria utenza il rispetto della normativa in materia di protezione dei minori e diritto all'istruzione

CAPITOLO 1 - INTRODUZIONE AL DOCUMENTO DI E-POLICY

1.1 - Scopo dell'e-Policy

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse.

Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E- policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali. Nello specifico:

- 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 digita

1.2 Ruoli e responsabilità

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.
Dirigente scolastico:

- Garantisce la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i

membri della
comunità scolastica;

- Garantisce ai propri docenti una formazione di base sulle tecnologie dell'Informazione e della Comunicazione
  (ICT) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse;
- Garantisce l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on- line;
- informa tempestivamente, qualora venga a conoscenza di atti di cyberbullismo
  che non si configurino come reato, i genitori dei minori coinvolti; (o chi ne
  esercita la responsabilità genitoriale o i tutori)
- Regola il comportamento degli studenti ed impone sanzioni disciplinari in caso di comportamento inadeguato.

TEAM Cyberbullismo d'Istituto:

- Coordina iniziative di prevenzione e contrasto del cyberbullismo messe in atto dalla scuola;
- Predispone un documento di rilevazione di incidenti di sicurezza in rete;
- Facilita la formazione e la consulenza di tutto il personale.

Animatore digitale e Team dell'innovazione:

- Pubblicano il presente documento di E-Safery Policy sul sito della scuola;
- Diffondono i contenuti del documento tra docenti e studenti.

Insegnanti:

- Provvedono personalmente alla propria formazione/aggiornamento sull'utilizzo del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in internet e dell'immagine degli altri: lotta al cyberbullismo);
- Supportano gli alunni nell'utilizzo consapevole delle tecnologie informatiche utilizzate a scopi didattici;
- Segnalano al Dirigente Scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazione;
- Supportano ed indirizzano alunni coinvolti in problematiche legate alla rete.

Tecnico informatico:

- Può controllare ed accedere a tutti i file della intranet;
- È l'unico a poter istallare nuovi software;
- Limita attraverso un proxy l'accesso ad alcuni siti;
- Coordina la prenotazione dei laboratori informatici consentendo di tenere traccia di ora e laboratorio utilizzati da ciascuno.

Direttore dei Servizi Generali e Amministrativi:

- Assicura, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione necessari ad evitare un cattivo funzionamento della dotazione Tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza

vengano rispettate.

Genitori:

- Contribuiscono, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- Incoraggiano l'impiego delle ICT da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga in sicurezza;
- Agiscono in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite;
- Rispondono per gli episodi commessi dai figli minori a titolo di culpa in educando (articolo 2048 del Codice Civile). Sono esonerati da responsabilità solo se dimostrano di non aver potuto impedire il fatto. Nei casi più gravi i giudici per l'inadeguatezza dell'educazione impartita ai figli emerge dagli stessi episodi di bullismo, che per le loro modalità esecutive dimostrano maturità ed educazione carenti.

1.3 - Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

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

L'E-policy viene condivisa e comunicata al personale, agli studenti e alle

studentesse, alla comunità scolastica attraverso:

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

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene pubblicato sul sito e sulla bacheca argo

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

1.5 - Gestione delle INFRAZIONI alla e-Policy

La scuola gestisce le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

- Richiamo verbale;
- Sanzioni estemporanee commisurate alla gravità della violazione commessa (assegnazione di attività aggiuntive da svolgere a casa sui temi di Cittadinanza e Costituzione);
- Nota informativa ai genitori o tutori mediante registro elettronico;
- Convocazione dei genitori o tutori per un colloquio con l'insegnante;
- Convocazione dei genitori o tutori per un colloquio con il Dirigente Scolastico.

Denunce di bullismo On-line saranno trattate in conformità con la legge.

1.6 - INTEGRAZIONE dell'e-Policy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida del Miur e le indicazioni normative generali sui temiin oggetto

1.7 - Monitoraggio DELL'IMPLEMENTAZIONE della e-Policy e suo aggiornamento

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

Netiquette d'Istituto

Al fine di prevenire comportamenti inappropriati o scorretti in costanza dell'utilizzo delle nuove tecnologie e durante le attività sincrone ed asincrone, l'Istituto si è dotato di un codice di condotta e di buone prassi racchiuso nella Netiquette che sottende allo svolgimento delle attività didattiche in DAD e in DDI; sono stati altresì deliberati il Piano ed il Regolamento DDI. La cittadinanza digitale si attua anche attraverso la promozione della cultura del rispetto di regole comuni nell'uso dei servizi telematici e dello sviluppo di regole di buon comportamento riferite specialmente ai Social Network e alla conoscenza delle condizioni del loro utilizzo.

Oltre che alla Netiquette d'Istituto si rimanda al documento approvato dalla Registration Authority Italiana-che fornisce delle indicazioni su etica e norme di buon uso dei servizi.

CAPITOLO 2 - FORMAZIONE E CURRICOLO

L'impiego corretto e consapevole delle TIC costituisce un fattore di innovazione della didattica e può utilmente contribuire all'aumento della motivazione e del rendimento degli studenti e alla modifica delle pratiche tradizionali di insegnamento: è quindi importante coglierne le potenzialità rispetto a contesti e finalità specifici. Per sostenere questo processo all'interno della scuola è necessario investire sulla formazione e l'aggiornamento degli insegnanti, soprattutto in relazione alla didattica per competenze e all'innovazione metodologico- didattica.

2.1.CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI

Il concetto di competenza rappresenta la capacità di utilizzare conoscenze, abilità e, in genere, tutto il proprio sapere, in situazioni reali di vita e lavoro. Le competenze digitali rientrano tra le otto competenze chiave che la Comunità Europea ha individuato per il pieno sviluppo della cittadinanza (Raccomandazioni del Parlamento Europeo e del Consiglio "Le competenze chiave per l'apprendimento permanente", 2006). La competenza digitale è una competenza trasversale, quindi tutti i docenti sono chiamati a promuoverla, come si evince dal profilo delle competenze in uscita dalla scuola secondaria inferiore. L'obiettivo è quello di rispondere ai bisogni di conoscenza, di espressione e di comunicazione dei ragazzi e aiutarli a organizzare, riflettere, attribuire senso alla loro esperienza tecnologica, orientarsi per una nuova ecologia dei media verso la logica dell'integrazione, della non intrusività del mezzo, dell'uso non passivizzante della tecnologia, di una esperienza tecnologica consapevole.
In quest'ambito si seguono le indicazioni contenute nel PNSD (azione 14), in cui si individuano alcuni framework di riferimento per la definizione e lo sviluppo delle

competenze digitali, tra cui il framework DIGCOMP, che prevede 21 competenze, di cui alcune specifiche nell'area della sicurezza.

Da qui la necessità di dotare il nostro Istituto di un Curricolo Digitale ossia di un percorso didattico progettato per sviluppare competenze digitali, di facile replicabilità, utilizzo e applicazione e necessariamente verticale. Partendo dal quadro di riferimento DIGCOMP è stato elaborato un curricolo digitale verticale nel quale sono elencate le competenze da considerarsi come traguardi in uscita dalla classe V scuola primaria e dalla classe terza scuola secondaria di primo grado. Relativamente alla scuola dell'infanzia il percorso delineato prevede un approccio esclusivamente ludico.

Nel rispetto delle azioni di prevenzione volte a promuovere e a preservare lo stato di salute e ad evitare l'insorgenza di patologie e disagi, l'IISS Don Michele Arena terrà in considerazione l'articolazione di prevenzione su tre livelli elaborata dall'OMS:

1. Prevenzione primaria o universale, le cui azioni si rivolgono a tutta la popolazione. Nel caso del bullismo, esse promuovono un clima positivo improntato al rispetto reciproco e un senso di comunità e convivenza nell'ambito della scuola.
2. Prevenzione secondaria o selettiva, le cui azioni si rivolgono in modo più strutturato e sono focalizzate su un gruppo a rischio, per condizioni di disagio o perché presenta già una prima manifestazione del fenomeno.
3. Prevenzione terziaria o indicata, le cui azioni si rivolgono a fasce della popolazione in cui il problema è già presente e in stato avanzato. Nel caso del bullismo la prevenzione terziaria si attua in situazioni di emergenza attraverso azioni specifiche rivolte ai singoli individui e/o alla classe coinvolta negli episodi di bullismo. Gli episodi conclamati sono anche definiti "acuti". Le azioni di prevenzione terziaria vengono poste in essere da unità operative adeguatamente formate dalla scuola come il Team Antibullismo e i professionisti dello sportello ascolto.

Nell'ambito della Prevenzione primaria o universale, in cui la principale finalità è promuovere la consapevolezza e la responsabilizzazione tra gli studenti, nella scuola e nelle famiglie, si attiveranno iniziative indirizzate a:

- accrescere la diffusa consapevolezza del fenomeno del bullismo e delle prepotenze a scuola attraverso attività curriculari incentrate sul tema (letture, film video, articoli, etc.);
- responsabilizzare il gruppo classe attraverso la promozione della consapevolezza emotiva e dell'empatia verso la vittima, nonché attraverso lo sviluppo di regole e di "politiche scolastiche";
- impegnare i ragazzi in iniziative collettive di sensibilizzazione e individuazione di strategie appropriate per la prevenzione dei fenomeni di bullismo e cyberbullismo,

come, ad esempio, Hackathon (a diversi livelli, d'istituto, di rete, provinciali, regionali) che hanno la capacità di mobilitare le migliori energie dei ragazzi, facendo loro vivere esperienze positive di socializzazione, con la contestuale valorizzazione delle competenze di cittadinanza e della loro creatività;

- organizzare dibattiti sui temi del bullismo e cyberbullismo, per sollecitare i ragazzi ad approfondire con competenza i temi affrontati e a discuterne, rispettando le regole della corretta argomentazione. Tali diversi approcci possono essere tra loro integrati, con l'obiettivo di accrescere l'attenzione sul tema e aiutare le ragazze e i ragazzi a costruire una scuola libera dal bullismo.

In tema di Prevenzione secondaria o selettiva si lavorerà su eventuali situazioni a rischio predisponendo sia una valutazione accurata dei problemi (incidenza dei fenomeni di bullismo e cyberbullismo e di altri segnali di disagio personale e familiare) sia un piano di intervento in collaborazione con i servizi del territorio, che coinvolga i ragazzi, gli insegnanti e le famiglie con un approccio sistematico, al fine di promuovere un percorso di vicinanza e ascolto e intercettare precocemente le difficoltà.

A proposito di Prevenzione terziaria o indicata per poter rilevare i casi acuti o di emergenza la scuola attiverà un sistema di segnalazione tempestiva. È utile inoltre una valutazione approfondita in funzione della gravità del problema, attraverso quattro specifici passaggi:

1. raccolta della segnalazione e presa in carico del caso;
2. approfondimento della situazione per definire il fenomeno;
3. gestione del caso con scelta dell'intervento o degli interventi più adeguati da attuare (individuale, educativo con il gruppo classe, di mantenimento e ripristino della relazione, intensivo e a lungo termine, di coinvolgimento delle famiglie);

monitoraggio della situazione e dell'efficacia degli intervento

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

L'Istituto ha aderito alle attività formative, promosse dal MIUR nell'ambito del PNSD, organizzate dagli snodi formativi e rivolte all'animatore digitale, al team per l'innovazione. Si prevede l'attivazione di iniziative di formazione facendo ricorso a soggetti esterni e/o al personale docente interno alla scuola che abbia acquisito competenze sull'innovazione didattica. Il percorso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica deve diventare un processo permanente che deve prevedere anche momenti di autoaggiornamento, di formazione personale o collettiva.

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

Coerentemente con quanto previsto dal PNSD, l'Istituto si avvale dell'Animatore Digitale, che coordina la diffusione dell'innovazione digitale e collabora con tutti i soggetti che possono contribuire alla realizzazione degli obiettivi del Piano. Anche il percorso della formazione specifica dei docenti sull'utilizzo consapevole e sicuro di INTERNET prevede momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi. Sono diffuse informazioni circa opportunità formative esterne in presenza e/o a distanza. Si prevede, inoltre, la promozione di attività formative interne (seminari, workshop, caffè digitali, ecc.), avvalendosi di risorse interne e/o esterne. Il docente referente partecipa a specifiche iniziative di formazione dedicate alla prevenzione e contrasto del bullismo e cyberbullismo.

2.4. - Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Il nostro Istituto ha organizzato incontri on line aperti alle famiglie e agli studenti tenuti dalla dott.ssa Arnone, psicologa d'Istituto, per sensibilizzare docenti, alunni e genitori sui temi della sicurezza online. 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, tra cui guide in formato pdf e video dedicati alle famiglie 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

CAPITOLO 3

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

3.1 - Accesso a Internet e filtri per la navigazione

L'Istituto dispone dell'accesso alla rete wi-fi. La rete è dotata di un firewall per la prevenzione dagli accessi dall'esterno nonché di filtri dei contenuti attraverso l'utilizzo di blacklist e parole chiave in continuo aggiornamento.

3.2 - Gestione accessi (password, backup, etc.)

La rete wi-fi è protetto da password in possesso esclusivo dei docenti che utilizzano quotidianamente i computer all'interno delle classi.

Le operazioni di gestione, configurazione, backup e ripristino sono affidate all'animatore digitale e a risorse tecniche interne presenti nell'Istituto.

3.3 - E-mail

Tutti i docenti dell'istituto possiedono una e-mail della scuola del tipo: nome.cognome@1circoloscafati.edu.it. Gli alunni, per l'utilizzo delle attività didattiche in DaD sono dotati di un indirizzo di posta elettronica della scuola del tipo:nome.cognome@1circoloscafati.edu.it. La dotazione di indirizzi di posta elettronica sia dei docenti che degli alunni appartiene all'infrastruttura delle Google Suite for Education.

3.4 - Sito web della scuola

Il sito web della scuola è gestito da un team preposto che si adopera affinché il sito sia sicuro e accessibile; ha cura di effettuare sia aggiornamenti e backup periodici che intervenire in caso di emergenza.

3.5 - Protezione dei dati personali

Ogni docente è responsabile del proprio username e della propria password di accesso al registro elettronico. In caso di smarrimento o dimenticanza i docenti devono rivolgersi alla segreteria e far presente il problema. A tutto il personale, docente e non docente, è stato

raccomandato di non salvare le password nei browser se gli strumenti vengono utilizzati da più persone e di effettuare sempre il logout dai siti a cui si accede con login e dalle caselle di posta personali. In ogni caso è consigliata la navigazione in modalità incognito del browser sulle periferiche della scuola (PC, notebook, tablet, ecc.). Si invitano altresì i docenti ad una custodia responsabile di tutte le credenziali di accesso con password segrete, alfanumeriche e sicure, cambiate almeno ogni tre mesi.

3.6 - Laboratori informatici

L'Istituto è dotato di tre laboratori informatici nei quali è presente una reta LAN cablata che utilizza le stesse protezioni firewall e regole di filtraggio della rete wi-fi.

CAPITOLO 4 - RISCHI ON LINE: CONOSCERE,PREVENIRE E RILEVARE

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 ma è altrettanto importante sapere quali sono le possibilistrategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano

L'Istituto così intende intervenire per la sensibilizzazione e prevenzione.

SENSIBILIZZAZIONE:

a partire dalle classi quinte della scuola primaria sino all'intero ciclo della secondaria, si punta a informare ma soprattutto ad educare alla consapevolezza e alla riflessione sulle seguenti tematiche:

- Uso o abuso di internet
- Quanto sono dipendente dallo smartphone, che uso ne faccio, per quante ore nell'arco della giornata, riesco a darmi delle regole?
- Come la rete ha modificato il mio modo di comunicare e di pormi in relazione con l'altro; i gruppi whatsapp, la messaggistica sostituiscono il linguaggio verbale e non verbale?
- Quanto sono consapevole dei pericoli della rete, cosa penso di sapere, come penso di evitarli

PREVENZIONE:

oltre a promuovere le competenze previste dal curriculo digitale un accento particolare viene dato:

- alla conoscenza dell'importanza di tutelare la propria privacy e quella degli altri (dati sensibili, password, foto, video) e dell'implicazioni legali in caso di trasgressione;
- alla conoscenza delle regole o norme etiche da tenere in mente quando si naviga in rete, quando si pubblica e/o si condivide un

contenuto;

- alla riflessione di come sia possibile dietro uno schermo, protetti dall'anonimato infrangere confacilità tali norme, essere vittime o artefici di azioni lesive e offensive della propria e altrui persona.

4.2 CYBERBULLISMO: CHE COS'È E COME PREVENIRLO

La legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", nell'art. 1, comma 2, definisce il cyberbullismo:

"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo"

Come previsto dalla legge, l'Istituto ha:

- Nominato un team che si occupa della prevenzione e del contrasto del bullismo e cyberbullismo
- Stipulato un regolamento antibullismo-cyberbullismo. Il regolamento include una parte dedicata all'uso di Internet in cui gli studenti si impegnano a:
  - utilizzare la rete nel modo corretto
  - rispettare le consegne dei docenti
  - non scaricare materiali e software senza autorizzazione
  - non utilizzare unità removibili personali senza autorizzazione
  - tenere spento lo smartphone al di fuori delle attività didattiche che ne prevedano l'utilizzo
  - durante le attività che prevedono lo smartphone, utilizzarlo esclusivamente per svolgere le attività didattiche previste
- Previsto una scheda di segnalazione di eventuali atti di bullismo e/o cyberbullismo.
- Individuato le procedure di intervento in caso di segnalazione.
- Pubblicato sul sito della scuola, a conoscenza delle famiglie e di tutti gli alunni, tale regolamento, incluso la scheda di segnalazione che può essere compilata e inviata via mail o consegnata in formato cartaceo nel piano della segreteria.
- Sempre sul sito è altresì pubblicato una guida per i genitori, con riferimenti di siti, servizi, numeri telefonici per un supporto psicologico e legale in caso di problematiche legate al bullismo e/o cyberbullismo. In questa guida sono indicati i segnali generali che può manifestare la vittima.

Le tipologie di cyberbullismo maggiormente considerate sono:

- Hate speech (il fenomeno dell'incitamento all'odio, all'intolleranza verso un gruppo o una persona.
- Dipendenza da internet e dal gioco online (i comportamenti patologici/dipendenze).
- Sexting (scambio di contenuti mediali sessualmente espliciti).
- 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).
- Denigration (diffusione di pettegolezzi, insulti, voci lesivi della dignità della persona).

Capitolo 5 - SEGNALAZIONE E GESTIONE DEI CASI

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, il Circolo Scafati I prevede strumenti di segnalazione ad hoc messi a loro disposizione

- un indirizzo e-mail specifico per le segnalazioni;
- sportello di ascolto con professionisti; docente referente per le segnalazioni.
- In allegato il modello di segnalazione utilizzata dall'Istituto per la segnalazione dei casi di bullismo e cyberbullismo.

L'Istituto ha costituito un Team, composto da 3 docenti/psicologi e il Dirigente, addetto alla presa in carico delle segnalazioni e alla messa in atto delle procedure delineate nel regolamento antibullismo-cyberbullismo, che in base alla gravità dell'atto segnalato possa prevedere collaborazioni con i servizi territoriali della Asl, Polizia, Servizi sociali.

Link utili:

https://www.generazioniconnesse.it/site/it/home-page/

https://azzurro.it/ (chat anonima o numero verde 1.96.96)

https://www.garanteprivacy.it/

https://www.iglossa.org/glossario/#B (l'ABC dei comportamenti devianti online)

https://www.commissariatodips.it/

Modello semplificato

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

Con questo modello si può richiedere al Garante per la protezione dei dati personali di disporre il blocco/divieto della diffusione online di contenuti ritenuti atti di cyberbullismo ai sensi dell'art. 2, comma 2, della legge 71/2017 e degli artt. 143 e 144 del Codice in materia di protezione dei dati personali, d. lg. n. 196 del 2003, come modificato dal decreto legislativo 10 agosto 2018, n. 101

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

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

CHI EFFETTUA LA SEGNALAZIONE?

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

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

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

(indicare una o più opzioni nella lista che segue)

- ☐ pressioni
- ☐ aggressione
- ☐ molestia
- ☐ ricatto

- ☐ ingiuria
- ☐ denigrazione
- ☐ diffamazione
- ☐ furto d'identità (es: qualcuno finge di essere me sui social network, hanno rubato le mie password e utilizzato il mio account sui social network, ecc.)
- ☐ alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali (es: qualcuno ha ottenuto e diffuso immagini, video o informazioni che mi riguardano senza che io volessi, ecc.)
- ☐ qualcuno ha diffuso online dati e informazioni (video, foto, post, ecc.) per attaccare o ridicolizzare me, e/o la mia famiglia e/o il mio gruppo di amici

QUALI SONO I CONTENUTI CHE VORRESTI FAR RIMUOVERE O OSCURARE SUL WEB O SU UN SOCIAL NETWORK? PERCHE' LI CONSIDERI ATTI DI CYBERBULISMO?
(Inserire una sintetica descrizione – IMPORTANTE SPIEGARE DI COSA SI TRATTA

DOVE SONO STATI DIFFUSI I CONTENUTI OFFENSIVI?

- ☐ sul sito internet [è necessario indicare l'indirizzo del sito o meglio l'URL specifico]
  _____

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

- ☐ altro [specificare] _____

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

1) _____
2) _____
3) _____

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

- ☐ Si, ma il titolare/gestore non ha provveduto entro i tempi previsti dalla Legge 71/2017 sul cyberbulllismo [allego copia della richiesta inviata e altri documenti utili]
- ☐ No, perché non ho saputo/potuto identificare chi fosse il titolare/gestore

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

☐ Si, presso _____;

☐ No

Luogo, data

Nome e cognome

Si ricorda che chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice in materia di protezione dei dati personali (Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante), salvo che il fatto non costituisca più grave reato

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Il Garante per la protezione dei dati personali (con sede in Piazza Venezia n. 11, IT-00187, Roma; Email: protocollo@gpdp.it; PEC: protocollo@pec.gpdp.it; Centralino: +39 06696771), in qualità di titolare del trattamento, tratterà i dati personali conferiti con il presente modulo con modalità prevalentemente informatiche e telematiche, per le finalità previste dal Regolamento (Ue) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196 e s.m.i.), in particolare per lo svolgimento dei compiti istituzionali nell'ambito del contrasto del fenomeno del cyberbullismo.

Il conferimento dei dati è obbligatorio e la loro mancata indicazione non consente di effettuare l'esame della segnalazione. I dati acquisiti nell'ambito della procedura di esame della segnalazione saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa.

I dati saranno trattati esclusivamente dal personale e da collaboratori dell'Autorità o delle imprese espressamente nominate come responsabili del trattamento. Al di fuori di queste ipotesi, i dati non saranno diffusi, né saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli ad altri soggetti coinvolti nell'attività istruttoria e nei casi specificamente previsti dal diritto nazionale o dell'Unione europea.

Gli interessati hanno il diritto di ottenere dal Garante, nei casi previsti, l'accesso ai propri dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (art. 15 e ss. del Regolamento). L'apposita istanza all'Autorità è presentata contattando il Responsabile della protezione dei dati presso il Garante (Garante per la protezione dei personali - Responsabile della Protezione dei dati personali, Piazza Venezia, 11, 00187, Roma, email: rpd@gpdp.it).