Ministero dell'Istruzione, dell'Università e della Ricerca
ISTITUTO COMPRENSIVO STATALE "E. PISCHEDDA"
SCUOLA INFANZIA – SCUOLA PRIMARIA – SCUOLA SECONDARIA I°GRADO
Via Verdi, 18 - 08042 BARI SARDO (NU)
TEL. +39.0782/223246
E Mail: nuic86200c@istruzione.it PEC: nuic86200c@pec.istruzione.it
Sito istituzionale: http://www.icbarisardo.edu.it
Codice Fiscale: 91005680912 – Codice Univoco Ufficio UFYLSG

Documento di ePolicy

NUIC86200C

I.C. BARI SARDO

VIA VERDI 18 - 08042 - BARI SARDO - NUORO (NU)

Aurelia Orrù

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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 digitali.

Argomenti del Documento

Perché è importante dotarsi di una E-policy?

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi

all'uso di Internet.

L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

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.

1.2.1 Il Dirigente Scolastico

Il Dirigente Scolastico garantisce la sicurezza online dell'intera comunità scolastica, promuove, in collaborazione con il referente del cyberbullismo, la cultura della sicurezza in rete. Ha la responsabilità della gestione dei casi di bullismo e cyberbullismo, di uso scorretto e/o improprio delle TIC.

1.2.2 Direttore dei Servizi Generali e Amministrativi

Il ruolo del direttore dei servizi generali e amministrativi include i seguenti compiti: assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura informatica della scuola sia funzionante, sicura e non aperta a uso improprio o a danno di 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 nell'ambito dell'utilizzo delle tecnologie digitali e di internet

1.2.3 Animatore Digitale

L'Animatore Digitale supporta il personale scolastico non solo dal punto di vista tecnico-informatico, ma anche sulla gestione dei rischi on-line, sulla protezione dei dati personali. Promuove momenti di formazione interna all'Istituto nell'ambito della scuola digitale (ad es.sviluppo delle competenze digitali previste anche nell'insegnamento dell'Educazione Civica). Ha il ruolo di monitorare e rilevare le problematiche connesse all'uso delle TIC (ad es. controllo degli accessi tramite password).

1.2.4 Il Referente del bullismo

Il Referente del bullismo ha il compito di promuovere e coordinare specifiche azioni per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine può

avvalersi della collaborazione dell Forze di Polizia, associazioni e centri di aggregazione sociale. Fondamentale è il suo ruolo in ambito scolastico ed extrascolastico nel coinvolgere colleghi, genitori e studenti.

Partecipa e cura la propria formazione che il MIUR fornisce su una apposita piattaforma

1.2.5 I Docenti

I Docenti hanno il ruolo di diffondere la cultura dell'uso responsabile delle TIC e della rete. Hanno il compito di 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. Accompagnano lo sviluppo delle competenze digitali degli studenti e vigilano sul corretto utilizzo delle TIC durante le lezioni in cui è programmato l'utilizzo di Internet. Segnalano al Dirigente Scolastico e/o al referente per il bullismo e cyberbullismo problemi, violazioni o abusi anche in online che vedano coinvolti gli studenti. Assicurano la riservatezza dei dati personali trattati ai sensi della normativa vigente

1.2.6 Il personale Amministrativo, Tecnico e Ausiliario (ATA)

Il personale 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. Diverse figure che, in sinergia, si occupano ciascuno per le proprie competenze, del funzionamento dell'Istituto Scolastico che passa anche attraverso lo sviluppo della cultura digitale e dell'organizzazione del tempo scuola. Il personale ATA deve, all'interno dei singoli regolamenti d'Istituto, essere coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

1.2.7 Gli Studenti

Gli studenti dovranno ascoltare e seguire le indicazioni fornite dai docenti per un uso corretto e responsabile delle tecnologie digitali, attuando le regole di *E-safety* per evitare situazioni di rischio e dovranno chiedere l'intervento dell'insegnante, o dei genitori a casa, nello svolgimento dei compiti per mezzo del digitale, qualora insorgano difficoltà o dubbi nel suo utilizzo. Dovranno comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi e adottare condotte rispettose degli altri anche quando si comunica in rete

1.2.8 I Genitori

I genitori avranno il ruolo di contribuire, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete. Dovranno

incoraggiare gli studenti ad un uso consapevole degli strumenti ITC nello svolgimento dei compiti a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza. Avranno il compito di lavorare in modo concorde con la Scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite. È estremamente importante che accettino e condividano quanto scritto nell 'EPolicy dell'Istituto.

1.2.9 Gli Enti educativi esterni e le associazioni Entrano in relazione con la scuola e devono conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC. Devono, inoltre, promuovere comportamenti sicuri e assicurare la protezione degli studenti e delle studentesse durante le attività svolte insieme.

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).

È importante garantire che tutti i soggetti esterni che erogano attività in ambito scolastico siano sensibilizzati e resi consapevoli dei rischi online che possono correre gli studenti e dei comportamenti corretti che devono adottare a scuola.

I soggetti esterni, qualora si verifichino episodi che mettano in pericolo gli studenti, devono rivolgersi all'insegnante di loro riferimento che ha l'obbligo di informare

tempestivamente il referente bullismo e cyberbullismo e il Dirigente. Tutti i soggetti esterni devono essere a conoscenza del documento di ePolicy e rispettarne i contenuti.

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

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/lle studenti/esse) si faccia a sua volta promotore del documento.

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 esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

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.

In particolare l'Istituto si impegna a:

- **Condividere e comunicare il documento agli alunni e alle alunne,** in questo modo si fornisce loro una base di partenza per un uso consapevole e maturo dei dispositivi e della tecnologia informatica. Tutti gli alunni avranno regole condivise di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici ed elementi per poter riconoscere e quindi prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e.
- **Condividere e comunicare il documento al personale scolastico** in modo da 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. Sarà fornita a a tutto il personale docente un'adeguata informazione/formazione sull'uso sicuro e responsabile delle TIC.

- **Condividere e comunicare il documento ai genitori** sul sito istituzionale della scuola, nonché tramite momenti di formazione specifici e durante gli incontri scuola-famiglia.

Tra le misure di prevenzione che la scuola metterà in atto vi saranno, inoltre, azioni finalizzate a promuovere una cultura dell'inclusione, del rispetto dell'altro e delle differenze così che l'utilizzo di Internet e dei cellulari, oltre che collocarci all'interno di un sistema di relazioni, ci renda consapevoli di gestire con un certo grado di trasparenza i rapporti che si sviluppano in tale ambiente, giungendo a riconoscere e gestire le proprie emozioni.

1.5 - Gestione delle infrazioni alla ePolicy

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

Disciplina degli Alunni

Qui di seguito viene fatta una elenco dei comportamenti potenzialmelnte sanzionabili per gli alunni/e.

La condivisione online di immagini o video di compagni/e senza il loro consenso o che li ritraggono in pose offensive e denigratorie;

La condivisione di scatti intimi e a sfondo sessuale;

La condivisione di dati personali;

L'invio di immagini o video volti all'esclusione di compagni/e.

Videoregistrare la lezione senza autorizzazione da parte del docente.

Riprendere immagini con l'uso del telefonino lo screen shot durante le videolezioni.

Sarà opportuno valutare la natura e la gravità dei comportamenti sanzionabili, al fine di considerare la necessità di denunciare l'episodio (con il coinvolgimento ad es. della Polizia Postale) o di garantire immediato supporto psicologico allo studente attraverso i servizi predisposti, qualora ciò fosse necessario.

A titolo esemplificativo, la scuola attuerà le seguenti azioni educative e/o sanzioni, valutando il grado 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.

Condotte e comportamenti assimilabili a cyberbullismo verranno vagliate e nel caso in cui nell'atto di cyberbullismo si configuri anche un'ipotesi di reato, potranno essere segnalate agli organi competenti.

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:

- 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 un'installazione di software o il salvataggio di materiali non idonei;
- 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 vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti.

La valutazione di ciascun caso spetta al Dirigente Scolastico in collaborazione con tutto il personale, il quale potrà fornire ogni informazione utile per l'analisi. A seconda dell'infrazione commessa, si terrà conto delle procedure previste dalla legge e dai contratti di lavoro.

1.6 - Integrazione dell'ePolicy 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 Miur e le indicazioni normative generali sui temi in oggetto.

Gli obiettivi previsti nel documento di Epolicy dovranno essere integrati anche nei seguenti documenti della scuola:

- Regolamento utilizzo del laboratorio di Informatica, delle postazioni di lavoro e dell'utilizzo di internet
- Regolamento utilizzo LIM e PC
- Regolamento uso dispositivi elettronici della scuola e/o personali

---

1.7 - Monitoraggio dell'implementazione della ePolicy 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.

Il monitoraggio dell'implementazione della Policy e del suo eventuale aggiornamento sarà svolta ogni anno. Tale monitoraggio sarà curato dal Dirigente Scolastico in collaborazione con il Gruppo di Lavoro e sarà rivolto agli insegnanti, al fine di valutare l'impatto della Policy e la necessità di eventuali miglioramenti.

Il nostro piano d'azioni

Azioni da svolgere nei prossimi 3 anni:

- Organizzare 1 evento di presentazione del progetto Generazioni Connesse e di presentazione e conoscenza dell'ePolicy rivolto ai docenti dell'Istituto.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse e di presentazione e conoscenza dell'ePolicy rivolto agli studenti.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse e di presentazione e conoscenza dell'ePolicy rivolto ai genitori.
- Organizzare uno o più eventi o attività volti a presentare il progetto

e consultare i docenti dell'Istituto per l'aggiornamento dell'ePolicy.

- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali".

Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa 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).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale.

L'Istituto si impegna a progettare e implementare un curricolo di competenze digitali che farà riferimento principalmente al Piano Scuola Digitale (PNSD), in particolar modo il paragrafo 4.2. su "Competenze e contenuti", al Sillabo sull'Educazione Civica Digitale, al DigComp 2.1 e alla Raccomandazione del Consiglio europeo relativa alle competenze chiave per l'apprendimento permanente (C189/9, p. 9).

L'Istituto individua 4 aree di competenza da sviluppare nel curricolo di competenze digitali in accordo con quelle individuate dal Digicomp 2.1:

Area 1: "Alfabetizzazione e dati".

L'area s'inquadra nella dimensione "informazionale" o "cognitiva" delle competenze digitali. Essa è relativa alla capacità di cercare, selezionare, valutare e riprocessare le informazioni in Rete. Nello specifico, per quest'area L'Istituto si impegna a sviluppare in bambini e ragazzi le seguenti competenze: 1. Navigare, ricercare e filtrare dati,

informazioni e contenuti digitali; 2. Valutare e gestire dati, informazioni e contenuti digitali; 3. Saper riconoscere e sapersi difendere da contenuti dannosi e pericolosi in Rete (es. app, giochi online, siti non adatti ai minori, materiale pornografico e pedo-pornografico etc.).

Area 2: “Comunicazione e collaborazione”.

Quest’area fa riferimento a quelle competenze volte a riconoscere le giuste ed appropriate modalità per comunicare e relazionarsi online: 1. Saper interagire con gli altri attraverso le tecnologie digitali; 2. Essere consapevoli nella condivisione delle informazioni in Rete; 3. Essere buoni “cittadini digitali”; 4. Collaborare adeguatamente con gli altri attraverso le tecnologie digitali; 5. Conoscere le “Netiquette”, ovvero le norme di comportamento online; 6. Saper gestire la propria “identità digitale”.

Area 3: “Creazione di contenuti digitali”.

Quest’area fa riferimento alle capacità di “valutare le modalità più appropriate per modificare, affinare, migliorare e integrare nuovi contenuti e informazioni specifici per crearne di nuovi e originali” (cfr. DigComp 2.1.). Le specifiche competenze digitali che si cercherà di sviluppare in questo caso sono: 1. Creare e modificare contenuti digitali in diversi formati per esprimersi attraverso mezzi digitali; 2. Modificare, affinare, migliorare e integrare informazioni e contenuti all’interno di un corpus di conoscenze esistente per creare conoscenze e contenuti nuovi, originali e rilevanti; 3. Capire come il copyright e le licenze si applicano ai dati, alle informazioni e ai contenuti digitali.

Area 4: “Sicurezza”.

Quest’area è parte di una dimensione più generale definita come “benessere digitale” che include la necessità di salvaguardare i propri dati personali e rispettare le regole nel trattare i dati altrui. Nello specifico, bisognerebbe puntare a sviluppare in bambini e ragazzi le seguenti competenze: 1. Imparare a proteggere i dispositivi e i contenuti digitali e comprendere i rischi e le minacce presenti negli ambienti digitali. Conoscere le misure di sicurezza e protezione e tenere in debita considerazione l’affidabilità e la privacy; 2. Proteggere i dati personali e la privacy negli ambienti digitali. Capire come utilizzare e condividere informazioni personali proteggendo se stessi e gli altri dai danni. Comprendere che i servizi digitali hanno un “regolamento sulla privacy” per informare gli utenti sull’utilizzo dei dati personali raccolti; 3. Conoscere (ed esercitare) i propri diritti in termini di privacy e sicurezza.

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 e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

La professione docente è complessa e pertanto richiede competenze diverse ed integrate, fra queste anche quelle di tipo digitale. Le TIC, infatti, dovrebbero essere usate dagli insegnanti ad integrazione della didattica al fine di progettare, sviluppare, utilizzare, gestire e valutare i processi di insegnamento e apprendimento di tutti gli studenti e le studentesse della classe, anche delle persone con disabilità (in chiave inclusiva).

Di conseguenza, gli insegnanti dovrebbero avere o raggiungere un buon livello di formazione in merito all'utilizzo e l'integrazione delle TIC nella didattica, partendo da compiti semplici (individuare i fabbisogni informativi; trovare dati, informazioni e contenuti attraverso una semplice ricerca in ambienti digitali) per arrivare a compiti più complessi (ricercare e filtrare portali e offerte).

Sulla base di tali premesse l'Istituto, anche attraverso il collegio dei docenti, promuove e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola (ad es. con l'aiuto dell'animatore digitale) dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dai docenti (anche online), purché restino coerenti con il piano di formazione.

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

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno

organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc…), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

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.

L'Istituto intende predisporre un'area specifica sul sito dell'Istituto con materiali formativi per gli insegnanti. Nella sezione, saranno messi a disposizione materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di Internet, prevedendo possibilità e modalità di condivisione fra gli insegnanti.

L'Istituto intende promuovere la formazione specifica legata al progetto Generazioni Connesse.

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

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle

tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

Il nostro Istituto ha organizzato negli anni passati diverse giornate sulla legalità in collaborazione con l'Arma dei Carabinieri, per sensibilizzare alunni e docenti anche sui temi della sicurezza online. L'obiettivo futuro è quello di estendere questi incontri anche ai genitori che devono essere parte attivia di questo percorso. Ci proponiamo nei prossimi anni di utilizzare questo approccio per sensibilizzare le famiglie, con incontri che offriranno un'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.

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.

Inoltre l'Isituto si impegnerà ad informare i genitori sulle condotte che si dovranno adottare a scuola e, in generale, offrire loro consigli da mettere in pratica con i propri figli, in particolare:

- **fornire ai genitori consigli e/o linee guida sull'uso delle tecnologie digitali nella comunicazione** con i figli e in generale in famiglia facendo riferimento alla sezione dedicata ai genitori del sito www.generazioniconnesse.it e facendone un richiamo ad essa anche sul sito web della scuola;
- **organizzare percorsi di sensibilizzazione e formazione dei genitori** su un uso responsabile e costruttivo della Rete in famiglia e a scuola.
- **prevedere azioni e strategie per il coinvolgimento delle famiglie** in tali percorsi di sensibilizzazione, ad esempio, mediante l'organizzazione di iniziative in cui anche gli studenti e le studentesse siano protagonisti.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020)

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi del fabbisogno formativo del corpo docente

sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi)

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- 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.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.
- Organizzare incontri con esperti per gli alunni/e sull'educazione alla cittadinanza digitale.

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

3.1 - Protezione dei dati personali

"Le scuole sono chiamate ogni giorno ad affrontare la sfida più difficile, quella di educare le nuove generazioni non solo alla conoscenza di nozioni basilari e alla trasmissione del sapere, ma soprattutto al rispetto dei valori fondanti di una società. Nell'era di Internet e in presenza di nuove forme di comunicazione questo compito diventa ancora più cruciale. È importante riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino".

(cfr. http://www.garanteprivacy.it/scuola).

Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta, tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali. Il "corretto trattamento dei dati personali" a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni.

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8), tutelato dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

Anche le scuole, quindi, hanno oggi l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, entrato in vigore lo scorso 19 settembre.

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare

riferimento all'uso delle tecnologie digitali, e indichiamo le misure che la scuola intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori. A tal fine, l'Istituto allega alla presente ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali.

Come disposto dal Regolamento UE 2016/679 (GDPR) artt. 13-14 e dal D.Lgs 196/2003 modificato dal D.lgs101/2018, per agevolare l'applicazione del GDPR il nostro istituto ha individuato come titolare del trattamento dei dati il Dirigente Scolastico dell'Istituto, mentre come responsabile per la Protezione dei Dati, nel seguito indicato sinteticamente come RPD, il rappresentale legale di Saema Informatica, Dott. Marco Cencetti.

La scuola ha adottato diversi protocolli per il trattamento dei dati personali di alunni e docenti in relazione all'adozione di strumenti per la didattica a distanza e all' utilizzo di strumenti di videocomunicazione durante le riunioni degli organi collegiali. L'Istituto predispone e comunica i modelli di liberatoria da utilizzare, conformi alla normativa vigente in materia di protezione dei dati personali. La scuola richiede alle famiglie la liberatoria per le riprese fotografiche e video.

3.2 - Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE

relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola".

Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

L'Istituto Comprensivo dispone dei strumentazione informatica quali potazioni informatiche e Lim collegata in buona parte dei plessi dell'istituto. Dispone di una rete informatica wi-fi e via cavo protetta da firewall sia per le attività didattiche che amministrative. La rete informatica della segreteria è separata da quella della didattica per una maggiore sicurezza.

L'assistenza tecnica del server e delle apparecchiature informatiche è affidata ad una ditta specializzata nel settore, che provvede al controllo sul backup dei dati, all'aggiornamento dei sistemi operativi e degli antivirus installati sulle macchine e al controllo del funzionamento del firewall.

L'utilizzo quotidiano del registro elettronico è gestito da Argo che ne garantisce la protezione dei dati, così come la normativa richiede. L'accesso alla strumentazione e alla connessione è consentito ai docenti solo ai fini didattici ed è normato da password. Gli studenti possono utilizzare la strumentazione e accedere alla rete internet solo per fini didattici e sotto stretto controllo del docente.

Tutti i docenti dell'istituto possiedono una e-mail della scuola del tipo: nome.cognome@icbarisardo.edu.it. Gli alunni, per l'utilizzo delle attività didattiche per la DaD sono dotati di un indirizzo di posta elettronica della scuola del tipo: nome.cognome@icbarisardo.edu.it. Gli indirizzi di posta elettronica sia dei docenti che degli alunni vengono utilizzati per l'accesso alla piattaforma didattica Mirosoft Teams.

L'Istituto, per garantire la sicurezza on line si impegna a attuare le seguenti azioni:

- Garantire formazione adeguata allo staff, incluso il corpo docenti;
- Testare regolarmente le possibili vulnerabilità;
- Preparare piani di azione in risposta ai problemi più seri;
- Predisporre la disconnessione automatica dei dispositivi, dopo un certo periodo di inutilizzo;

- Impostare il browser per l'eliminazione dei cookies in chiusura;
- Definire una policy sulle password utilizzate (password forti, non vulnerabili);
- Minimizzare i privilegi amministrativi nell'utilizzo dei software;
- Sviluppare il regolamento sull'uso delle tecnologie a scuola (policy di uso accettabile).

3.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

3.3.1 Sito WEB

l 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. La pubblicazione dei contenuti avviene rispettando tutti i protocolli relativi alla privacy e il Dirigente Scolastico ne è il garante.

La scuola non pubblica sul proprio sito materiale prodotto dagli alunni senza il permesso dei loro genitori; inoltre, le fotografie degli stessi sono pubblicate previa liberatoria dei genitori o tutori.

La scuola offre all'interno del proprio sito web i seguenti servizi alle famiglie ed agli utenti esterni:

- servizio del Registro on-line per comunicazione di voti e assenze e per prenotazione di colloqui individuali con i docenti
- segreteria digitale (pubblicazione delle circolari della Presidenza)
- consultazione elenchi libri di testo
- Piano Triennale dell'Offerta Formativa
- Regolamento di Istituto

3.3.2 Email Istituzionale

La scuola utilizza per le comunicazioni ai docenti e ai genitori la email d'istiuto nuic86200c@istruzione.it.

3.3.3 Registro Elettronico

La scuola utilizza per le comunicazioni ai docenti, agli studenti ai genitori il registro elettronico ARGO.

Docenti
Ad ogni docente è assegnata una login e password per la gestione del registro elettronico e posta elettronica dell'Istituto.
Ogni docente firma la presenza secondo l'orario scolastico e tiene aggiornato il registro personale.
L'Istituto non risponde dell'alterazione di eventuali dati.

Famiglie
I genitori accedono al Registro Elettronico con un profilo assegnato dal sistema, per la comunicazione sull'andamento didattico-disciplinare dell'alunno, per la prenotazione dei colloqui individuali e per prendere atto delle comunicazioni del Dirigente.

Dirigente, Collaboratori, Segreteria
La comunicazione formale con le famiglie avviene tramite l'invio dalle mail istituzionale della scuola alle mail personali dei genitori o tramite pubblicazione nella sezione BACHECA del registor elttronico.

3.3.4 Piattaforma per la Didattica Digitale Integrata

La scuola ha adottato per tutto il personale docente e gli studenti la piattaforma didattica *Microsoft Teams* che consente di comunicare, gestire e scambiare materiali con grande semplicità e velocità. Le app utilizzate garantiscono la privacy e la sicurezza.

Tutti gli studenti hanno accesso a:

- email personale con spazio di archiviazione llimitato;
- One drive che permette lo stoccaggio nel cloud di una gran mole di dati;
- Microsoft Teams dove avere una classe virtuale nella quale lavorare attivamente e ricevere
- materiale aggiuntivo dagli insegnanti;
- Pacchetto Microsoft office con tutte le principali apps per creare testi, presentazioni o fogli di calcolo.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

La presente ***ePolicy*** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

L'utilizzo delle TIC nella nostra scuola sarà regolamentato sia da un adeguamento del Regolamento d'istituto e del Patto di corresponsabilità sia dalla stesura di una netiquette per condividere le "buone pratiche" di utilizzo dei dispositivi digitali personali e non in modo da formare cittadini consapevoli e responsabili.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

Scegliere almeno 1 di queste azioni:

- 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

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).

Scegliere almeno 1 di queste azioni:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli
- studenti e delle studentesse
- 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 uno o più eventi o attività volti a consultare i docenti dell’Istituto per redigere o integrare indicazioni/regolamenti sull’uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull’uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell’Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell’Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell’Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell’Istituto sui temi dell’accesso ad Internet e dell’uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell’Istituto sui temi dell’accesso ad Internet e dell’uso sicuro delle tecnologie digitali (cybersecurity)

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 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.*

Per i ragazzi nativi digitali le interconnessioni tra vita e tecnologia sono la normalità. Essi, pur essendo spesso tecnicamente competenti, tendono a non cogliere le implicazioni dei loro comportamenti e tale fenomeno è tanto maggiore quanto è più forte il coinvolgimento emotivo nell'utilizzo dei nuovi media. La necessità di supportare gli alunni affinché abbiano un approccio positivo e consapevole delle TIC,

inteso come protezione dai rischi della rete ma anche come capacità di saper cogliere le opportunità insite in essa, induce la scuola e i genitori a non perdere di vista il proprio ruolo educativo, le proprie responsabilità. A tal fine la scuola deve promuovere azioni di Sensibilizzazione e Prevenzione, cioè informare sui rischi che potrebbero presentarsi in rete e fornire agli studenti gli strumenti idonei per prevenirli.

L'Isituto 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 con facilità tali norme, essere vittime o artefici di azioni lesive e offensive della propria e altrui persona

In considerazione dell'importanza di favorire la sinergia degli interventi educativi di Scuola e famiglia per il successo scolastico ed educativo di ogni studente, il presente documento è allegato al Patto Educativo di Corresponsabilità stipulato con le famiglie degli alunni quale l'impegno reciproco di scuola e famiglia alla corresponsabilità formativa, nella quale rientrano a pieno titolo i temi legati alla eSafety.

Allo scopo di mantenere viva l'attenzione delle famiglie sui tali temi, verranno inoltre valorizzate le opportunità di incontro e formazione per le famiglie sui temi oggetto della Policy, offerte dal territorio, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata.

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".

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 (ed ex 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.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
    - Ha 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.
    - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Il nostro Istituto si propone di dare piena attuazione alla recente normativa in materia di bullismo e cyber bullismo (legge 71/2017) e delle recenti linee guida sul bullismo e cyberbullismo - 2021 con l'obiettivo di contrastare tali fenomeni in tutte le loro manifestazioni.

Le azioni di prevenzione previste nell'utilizzo delle TIC adottate dall'Istituto sono le seguenti:

1. Valutazione degli studenti a rischio, osservazione del disagio, rilevazione dei comportamenti dannosi per la salute di ragazzi/e.

2. Formazione del personale scolastico, prevedendo la partecipazione ai moduli formativi previsti dalla piattaforma ELISA di almeno due docenti referenti per ogni scuola.

3. Attività di formazione/informazione rivolte a docenti, studenti, famiglie e personale ATA, sui temi dei regolamenti e delle procedure adottate dal referente per il bullismo e il cyberbullismo e dal Team Antibulllismo;

4. Rilevazione dei fenomeni di bullismo e cyberbullismo attraverso questionari e/o osservazioni sulla base della documentazione disponibile sulla piattaforma ELISA;

5. Attivazione di un sistema di segnalazione nella scuola;

6. Promozione e attivazione di uno sportello psicologico e di un centro di ascolto gestito da personale specializzato (psicologi presenti nell'istituto o nei servizi del territorio) anche in collaborazione con i servizi pubblici territoriali; ove non sia possibile attuare tali condizioni, si potrebbe favorire l'istituzione di un servizio condiviso da reti di scuole.

7. Costituire gruppi di lavoro che includano il/i referente/i per la prevenzione del bullismo e del cyberbullismo, l'animatore digitale e altri docenti impegnati nelle attività di promozione dell'educazione civica.

4.3 - Hate speech: che cos'è e come prevenirlo

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) 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.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

La scuola si propone, in un clima di convivenza civile, di far acquisire a tutti gli alunni attitudini di rispetto verso l'unicità di ciascuno, nell'accettazione dell'altro. Essa ha il dovere di creare e mantenere un ambiente sano e sereno, per facilitare lo studio e la crescita personale.

Occorre in tal senso fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, e promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network.

Pertanto il nostro Istituto inserirà nel PTOF un Progetto di Educazione alla Legalità aderendo alla Giornata dedicata al tema dei Diritti dell'Infanzia e dell'Adolescenza, a cui parteciperanno gli alunni dei tre ordini di scuola di tutti e tre i plessi con finalità specifiche di sviluppo delle competenze digitali e educazione ad un uso etico e consapevole delle tecnologie.

4.4 - Dipendenza da Internet e gioco online

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.

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale?

L'Istituto in tal senso vuole promuovere azioni di prevenzione attraverso percorsi sul

benessere digitale dedicando al tema un momento specifico e riflettendo con studenti e studentesse per fare in modo che la tecnologia sia strumento per raggiungere i propri obiettivi e non sia solo distrazione o addirittura ostacolo. Il compito della scuola sarà quello di integrare la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online. Si dovrà riflettere insieme su: come si trascorre il tempo on line? quando aggiunge valore alla vita e quando fa perdere tempo? quale atteggiamento si potrebbe cambiare quando si è online? che ruolo ha e deve avere la tecnologia (internet o il gioco) nella propria vita? Allo stesso modo quando parliamo di videogiochi, dobbiamo pensarli non in termini negativi ma di benessere digitale. Sono parte del mondo di studenti e studentesse. E, allora, riflettiamo insieme a ragazzi e ragazze su: quando sono una risorsa? Accedono a contenuti adeguati all'età? A che ora e per quanto tempo li usano? Diventa utile riflettere con i ragazzi e le ragazze rispetto all'uso della tecnologia in termini di qualità e tempo. Se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi.

Tra le azioni che l'Istituto intende portare avant c'è percorso di Gamification insieme agli alunni con la finalità di rendere gli alunni/e consapevoli dei rischi connessi ad un eccessivo utilizzo di Internet.

4.5 - Sexting

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/le ragazzi/e 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.

A livello preventivo, è importante che vengano attivati all'interno dell'istituto scolastico percorsi di formazione rivolti ai ragazzi, ai docenti e ai genitori per approfondire i rischi e le conseguenze di episodi di sexting. È importante offrire spunti per avviare il dialogo in classe con gli studenti, partendo da storie accadute o da fatti di cronaca da commentare per riflettere sui punti salienti:

- Consapevolezza del proprio valore e della propria immagine
- L'importanza di agire quanto prima, parlandone con una figura adulta
- Rispetto e responsabilità
- Forme sanzionatorie e di tutela

4.6 - Adescamento online

Il ***grooming*** (dall'inglese "groom" - curare, prendersi cura) rappresenta 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.

In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies – l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

L'Istituto mirerà a sensibilizzare gli alunni sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni carpendo la loro fiducia, approfondendo anche gli aspetti giuridici.

Pertanto la scuola, con l'aiuto dello specialista che si occupa dello Sportello di Ascolto Psicologico (già attiva tato durante il corrente anno scolastico) si propone di attivare incontri per ampliare la conoscenza di tale fenomeno e permettere agli alunni di raccontare le loro esperienze o casi di cui loro stessi sono a conoscenza, riponendo la fiducia nei loro docenti disponibili ad ascoltarli.

4.7 - Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) 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.

La legge n. 269 del 3 agosto 1998 *"Norme contro lo sfruttamento della*

prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella ***legge n. 38 del 6 febbraio 2006*** *"Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet"*, segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Secondo la Legge 172/2012 - *Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi 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.

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: 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).

Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children.

Anche per la pedopornografia vale quanto detto per gli altri rischi on line e la nostra scuola continuerà a percorrere la strada della prevenzione e sensibilizzazione mediante incontri formativi e percorsi laboratoriali. Anche in questo caso l'educazione all'affettività riveste un ruolo fondamentale nel processo di crescita educativa degli alunni. Nell'organizzazione degli incontri informativi la scuola si propone di coinvolgere tutto il personale della scuola e le famiglie. Essendo il tema della pedopornografia estremamente delicato, occorrerà parlarne sempre in considerazione

della maturità, della fascia d’età e selezionandoil tipo di informazioni che si possono condividere.

Il nostro piano d'azioni

AZIONI (da sviluppare nell’arco dei tre anni scolastici successivi).

Scegliere almeno 1 di queste azioni:

☐ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all’utilizzo delle tecnologie digitali, rivolti agli/lle allunni/alunne.

☐ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all’utilizzo delle tecnologie digitali, rivolti agli/lle alunni/alunne, con il coinvolgimento di esperti.

☐ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all’utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.

☐ Implementare attività relative alla consapevolezza nell'uso delle TIC e ai principi dell'Epolicy per le alunni e alunne all'interno del curricolo di Educazione Civica.

☐ Organizzare laboratori di educazione alla sessualità e all’affettività, rivolti agli/lle alunni/alunne.

☐ Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull’inclusione rivolti a genitori, allunni/alunne e personale della scuola.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire).

Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).

Nelle procedure:

- sono indicate le **figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso**.
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

Inoltre, la scuola **individua le figure che costituiranno un team** preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la **collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio** (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica.

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e

studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

A seguire, le problematiche a cui fanno riferimento le procedure allegate:

- **Cyberbullismo**: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online**: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting**: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per

segnalare la presenza di materiale pedopornografico online.

1. Contenuti afferenti alla privacy e non autorizzati (foto o video personali, l'indirizzo di casa o il telefono, informazioni private proprie o di altri, ecc.);

2. Contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto e video imbarazzanti, virus, contenuti razzisti o inneggianti al suicidio, immagini o video umilianti, insulti, ecc.);

3. Contenuti afferenti alla sessualità (messaggi molesti, conversazioni che connotano una
relazione intima, foto e video personali con nudità o abbigliamento succinto, immagine pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività
sessuali, ecc.).

5.2. - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

- CASO A (SOSPETTO) – Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.
- CASO B (EVIDENZA) – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

Per tutti i dettagli fate riferimento agli allegati con le procedure.

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, la scuola può prevedere alcuni 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 inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

1. In presenza di sospetto relativo a un episodio di cyberbullismo, basato su testimonianza diretta o diretta visione di prodotti informatici di tipo denigratorio o usati a tal fine (foto, post, video, ...), il docente, venuto a conoscenza dei fatti nell'esercizio delle proprie funzioni, in qualità di Pubblico Ufficiale (art. 357 c.p. e art. 331 c.p.p.), relaziona al Dirigente Scolastico per iscritto, avendo cura di far protocollare la propria segnalazione, da inoltrarsi preferibilmente a mano in busta chiusa. Il Dirigente deve comunicare per iscritto al docente avvenuta trasmissione all'autorità competente. Qualora ciò non avvenisse entro i due giorni lavorativi successivi al protocollo, il docente stesso dovrà inoltrare la segnalazione. In particolare, nei casi di reati perseguibili d'ufficio (per es. sexting, pedopornografia,adescamento on-line, ...) o in caso si sospetti grave pregiudizio per il minore, il docente, informato dei fatti, in qualità di Pubblico Ufficiale, denuncia immediatamente all'autorità di P.S. o all'autorità giudiziaria, dandone comunicazione al Dirigente Scolastico.
2. In caso sia individuata la vittima, il Dirigente Scolastico o, su delega, il Vicario e/o il Secondo Collaboratore, e/o il coordinatore di classe, e/o il referente per il bullismo o cyberbullismo,deve convocare i genitori (o chi esercita la responsabilità genitoriale) e informarli dei fatti, eventualmente con il supporto degli esperti dello sportello di ascolto. La convocazione dei genitori non deve essere fatta per i reati di sexting, pedopornografia o per altri reati in cui sia possibile che la vulnerabilità del minore nasca all'interno del nucleo familiare.
3. Gli studenti, che vivano in prima persona o come testimoni situazioni problematiche, possono rivolgersi ai docenti di classe, al coordinatore di classe, al Dirigente Scolastico, al referente per il contrasto del bullismo e del cyberbullismo, al referente dello sportello d'ascolto, a qualsiasi commissariato di P.S., al commissariato on-line https://www.commissariatodips.it/), alla Polizia Postale, all'Arma dei Carabinieri. Inoltre, gli studenti possono inviare la propria

segnalazione, anche in forma anonima, tramite l'applicazione YouPol della Polizia di Stato (https://www.poliziadistato.it/static/40/presentazione_youpol_-esserci.pdf.pdf).

4. In particolare, i minori che ritengano che determinanti contenuti a loro riferiti e diffusi per via telematica (foto e/o video imbarazzanti e/o offensivi, pagine web e/o post sui social network in cui si è vittime di minacce e/o offese e/o insulti, ecc.) siano atti di cyberbullismo, ne possono richiedere l'oscuramento, la rimozione o il blocco. Le richieste vanno inviate al titolare del trattamento o al gestore del sito o del social media dove sono pubblicati i contenuti ritenuti atti di cyberbullismo. L'istanza può essere inoltrata direttamente dal minore, se ha più di 14 anni, oppure da chi esercita la responsabilità genitoriale. Nel caso la richiesta non venga soddisfatta, ci si può rivolgere al Garante per la protezione dei dati personali, che, entro 48 ore, provvede in merito alla segnalazione (legge n 71/2017). Per inoltrare le segnalazioni si può utilizzare il modello disponibile su www.garanteprivacy.it/cyberbullismo, inviandolo via e-mail a cyberbullismo@gpdp.it.
5. Gli psicologi operanti all'interno dell'Istituto scolastico, gli addetti del personale ATA, gli esperti esterni coinvolti in attività di docenza per attività dell'Istituto (progetti, PCTO, corsi…), in sede o fuori sede, ricoprono il ruolo di Operatori Incaricati di Pubblico Servizio (art.358 c.p.) e come tali sono obbligati a denunciare e o segnalare i fatti appartenenti alle tipologie sopradescritte, di cui sono informati per testimonianza diretta o visione diretta di materiale che rientri nelle categorie di reati precedentemente indicati. Pertanto, sono tenuti a mettere in atto le procedure contenute nei precedenti paragrafi, comunicando, inoltre, per iscritto, al docente con cui abitualmente hanno contatti (referente di progetto, coordinatore di classe, docente della classe,…), i fatti di cui sono venuti a conoscenza e l'avvenuta segnalazione al Dirigente Scolastico e/o all'autorità di P.S. e/o all'autorità giudiziaria.
6. Il consiglio di classe a cui appartenga lo studente o il gruppo di studenti coinvolto nei fatti previa informativa da parte del titolare della segnalazione/denuncia o da parte del Dirigente Scolastico, attiva percorsi di informazione, prevenzione e sensibilizzazione, avvalendosi, se giudicato opportuno, del supporto di esperti esterni quali psicologi, servizi sociali, forze dell'ordine, Polizia Postale, ecc. E' fondamentale che venga rispettato il segreto d'ufficio sull'identità dei soggetti implicati, indipendentemente dal loro ruolo. Il consiglio di classe e, a seconda della gravità della violazione, il Consiglio d'Istituto valutano l'eventuale erogazione di provvedimenti o sanzioni disciplinari nelle sedi, nelle modalità e con le finalità previste dal Regolamento d'Istituto e dallo Statuto degli Studenti e delle Studentesse.
7. In tutte queste procedure, gli studenti, le famiglie, il personale ATA, gli esperti esterni, i docenti e il Dirigente Scolastico possono avvalersi della figura del referente per il contrastoal bullismo e al cyberbullismo.

5.3. - Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni**: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico**: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

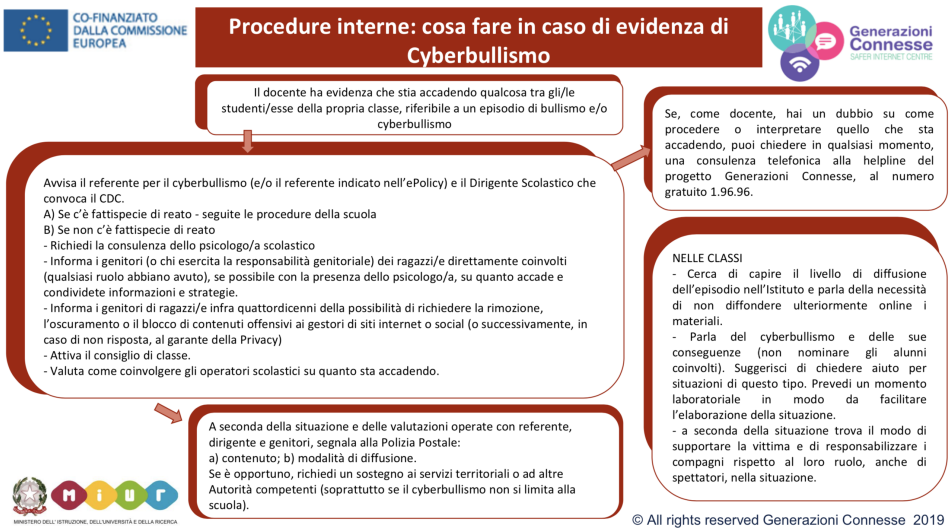
Tra gli attori sul territorio deputati alla presa in carico dei vari aspetti che una

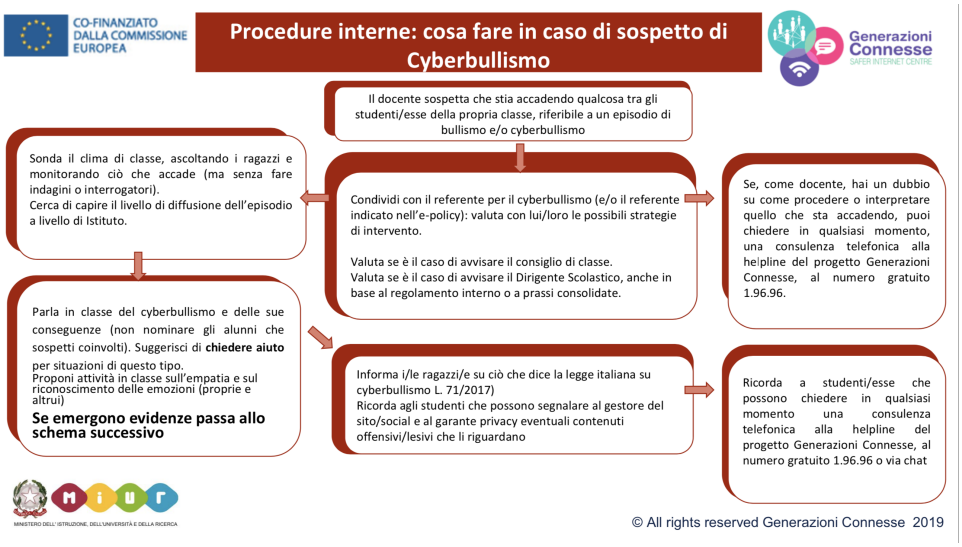
problematica legata ad un utilizzo delle TIC può presentare ricordiamo anche:

- Servizi Socio Assistenziale Unione Comuni d'Ogliastra **email:** servizisociali@doc.unionecomunidogliastra.it;
- Comando Stazione Carabinieri Bari Sardo e Cardedu **telefono** 0782 29522 / 0782 75822;
- Commissariato di Polizia di Tortolì **telefono:** 0782600000 - **email:** comm.tortoli.nu@pecps.poliziadistato.it
- Questura di Nuoro **telefono:** 0784214111 - **email:** gab.quest.nu@pecps.poliziadistato.it;
- Procura della Repubblica di Nuoro **email**: procura.nuoro@giustizia.it;

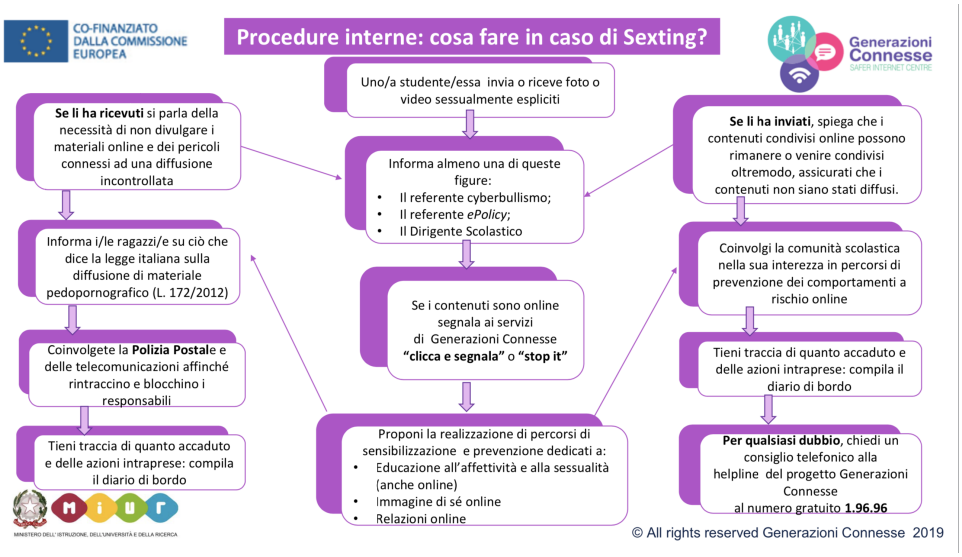
5.4. - Allegati con le procedure

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?

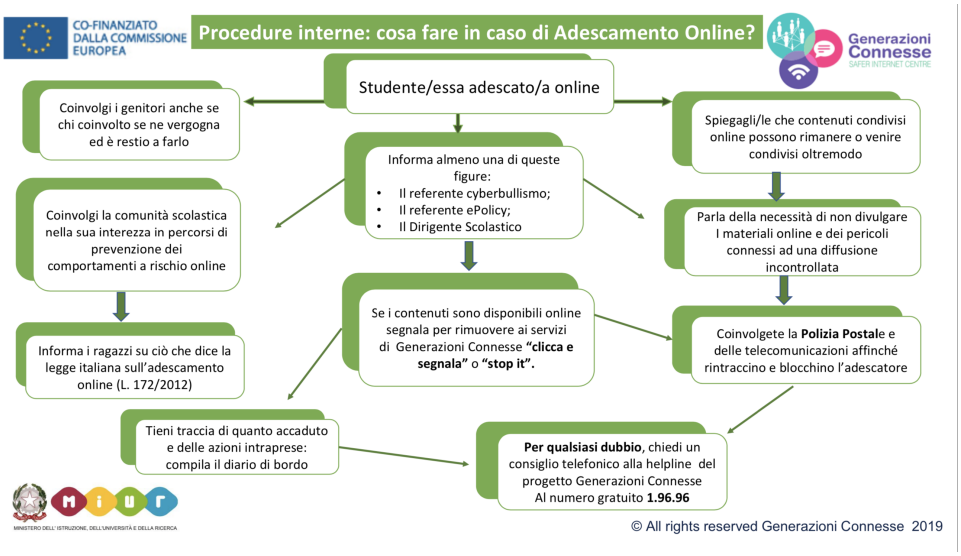




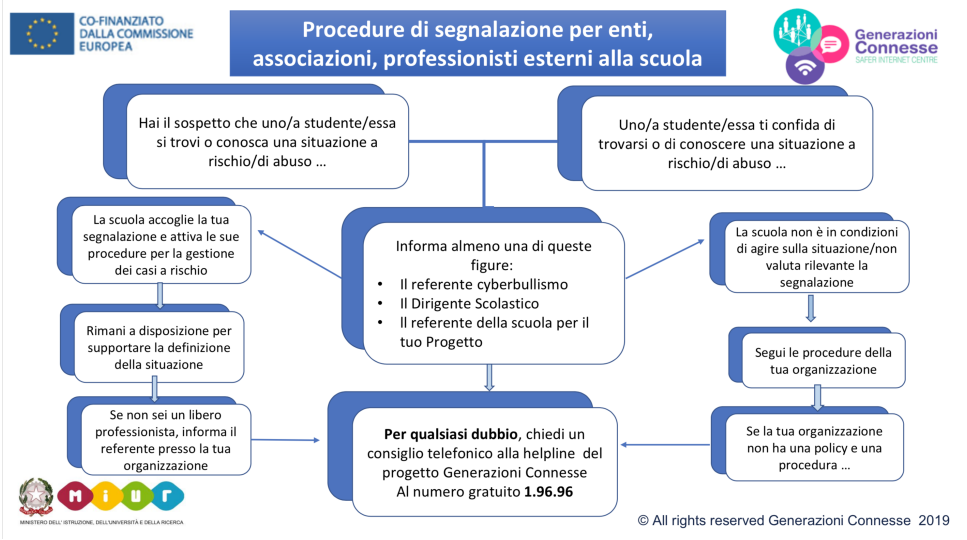
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola



Altri allegati

- Scheda di segnalazione
- Diario di bordo
- iGloss@ 1.0 l'ABC dei comportamenti devianti online
- Elenco reati procedibili d'ufficio

Le procedure allegate saranno oggetto di verifica sul campo nei prossimi anni scolastici.

Il nostro piano d'azioni

- Ridefinizione del Regolamento d'Istituto e del Patto di Corresponsabilità in funzione dei principi individuati nell'Epolicy;;
- Creazione sul sito di una sezione dedicata alle procedure di segnalazione di violazione e alla modulistica specifica, con indicazione dei principali Enti e Servizi a cui rivolgersi per assistenza e tutela;
- Informativa alle famiglie sulla presenza di incontri dedicati al tema del cyberbullismo tenuti sul territorio e in collaborazione con i servizi minorili dell'Amministrazione della Giustizia, le Prefetture, gli enti locali, i servizi territoriali, le forze di Polizia ed enti o associazioni dedicati.