Documento di ePolicy

AGIS01600N

IIS - DON MICHELE ARENA

VIA NENNI - 92019 - SCIACCA - AGRIGENTO (AG)

Capitolo 1 - Introduzione al documento di ePolicy

- 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

1. **Presentazione dell'ePolicy**
    1. Scopo dell'ePolicy
    2. Ruoli e responsabilità
    3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
    4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
    5. Gestione delle infrazioni alla ePolicy
    6. Integrazione dell'ePolicy con regolamenti esistenti
    7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
2. **Formazione e curricolo**
    1. Curricolo sulle competenze digitali per gli studenti
    2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
    3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
    4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
    1. Protezione dei dati personali
    2. Accesso ad Internet
    3. Strumenti di comunicazione online
    4. Strumentazione personale
4. **Rischi on line: conoscere, prevenire e rilevare**
    1. Sensibilizzazione e prevenzione
    2. Cyberbullismo: che cos'è e come prevenirlo
    3. Hate speech: che cos'è e come prevenirlo
    4. Dipendenza da Internet e gioco online
    5. Sexting
    6. Adescamento online
    7. Pedopornografia
5. **Segnalazione e gestione dei casi**
    1. Cosa segnalare
    2. Come segnalare: quali strumenti e a chi
    3. Gli attori sul territorio per intervenire
    4. Allegati con le procedure

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.

L'E-Policy è un documento programmatico autoprodotto dalla scuola volto a promuovere le competenze digitali e l'uso delle tecnologie digitali in modo positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo.

L'E-policy che l'IISS "Don Michele Arena" rinnova ed integra, alla luce e in attuazione delle Linee di Orientamento 2021 per la prevenzione e il contrasto del Bullismo e Cyberbullismo- di cui alla nota n.482 del 18.02.2021 -Ministero dell'Istruzione, è uno strumento con cui definisce e condivide:

- il proprio approccio alle tematiche legate alle competenze digitali, alla sicurezza online e ad un uso positivo delle tecnologie digitali nella didattica;

- le norme comportamentali e le procedure per l'utilizzo delle Tecnologie dell'informazione e della comunicazione (TIC) in ambiente scolastico;

- le misure per la prevenzione;

- le misure per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

Internet rappresenta un'ottima opportunità per fare ricerca, comunicare, documentare il proprio lavoro, pubblicare elaborati, condividere risorse ed esperienze. L'IISS "Don Michele Arena", anche a seguito dell'emergenza sanitaria che ha indirizzato verso forme alternative alla tradizionale didattica in presenza (DAD-DDI), ha potenziato l'uso delle tecnologie informatiche nella didattica e nell'organizzazione generale della scuola sia per svolgere le attività didattiche e le esperienze formative, sia per condurre in modo più efficiente le funzioni amministrative, anche con il ricorso allo smart working. Gli strumenti informatici però, oltre a fornire un'enorme opportunità espongono gli utenti, in particolar modo i minori ed i soggetti con limitate competenze informatiche, ad alti rischi che sono tanto più elevati quanto più è alto il grado di inconsapevolezza dei modi legittimi di usare la rete stessa. Al fine di promuovere l'acquisizione della consapevolezza dell'uso legittimo della rete e per far sì che internet possa solo avvantaggiare i giovani, il nostro Istituto aderisce al progetto "Generazioni Connesse" e rinnova l'E-Safety Policy che traccia le linee guida per un uso sicuro delle nuove tecnologie

È in atto l'aggiornamento e l'implementazione costante del sito web istituzionale attraverso cui la scuola comunica al territorio le proprie iniziative, garantendo l'accesso alla documentazione necessaria ad una partecipazione attiva da parte degli

utenti in modo chiaro e tempestivo. Il nostro Istituto attualmente utilizza la piattaforma G.suite for education avendo registrato il proprio dominio @iissarena.edu.it; all'interno di quest'area vengono create classi virtuali (google classroom) in cui gli studenti e i docenti possono comunicare in modo sicuro e protetto.

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'IISS "Don Michele Arena"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.

Principi generali

L'IISS "Don Michele Arena", con riguardo all'etica e al buon uso dei servizi in rete, si attiene ai seguenti principi generali:

1. internet bene comune, internet strumento cruciale per lo sviluppo e l'esercizio dei diritti umani, neutralità della rete e architettura aperta, benefici della tecnologia e della rete, modello decisionale trasparente con il coinvolgimento di tutti i portatori di interesse (stakeholder);

2. Cittadinanza in rete: accesso all'infrastruttura indipendentemente dal luogo di residenza, punti di accesso ad internet, accesso e riutilizzo dei dati del settore pubblico, accessibilità come strumento di inclusione, diritti umani e libertà fondamentali in rete e per mezzo della rete, auto-organizzazione e autonomia degli individui in rete;

3. Consumatori e utenti della rete: competenze digitali, identità digitale, riservatezza, accesso, archiviazione e cancellazione dei dati personali;

4. Produzione e circolazione dei contenuti: condivisione dei contenuti e della conoscenza in rete, proprietà intellettuale in ambiente digitale;

5. Sicurezza in rete: infrastrutture di interesse nazionale, sicurezza in rete, internet, comunicazione di crisi e operazioni di soccorso, protezione dei soggetti deboli.

Interventi a molteplici livelli

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);

4. monitoraggio della situazione e dell'efficacia degli interventi

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.

- 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.

Nell'ambito di questa policy sono individuati i seguenti ruoli e le principali responsabilità correlate:

RUOLI RESPONSABILITA'

1. dirigente scolastico

Deve:
• Garantire la sicurezza online dei membri della comunità scolastica;
• Accertarsi che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro e delle differenze, un utilizzo positivo e responsabile delle TIC;
• Assicurare che il sito web della scuola includa informazioni sulla cultura della sicurezza online, rilevanti e condivise con i diversi stakeholders
• Promuove le migliori pratiche nella gestione delle informazioni, ossia mette in atto un sistema di controllo di accesso appropriato. I dati sono utilizzati, trasferiti e cancellati in linea con i requisiti di protezione dei dati;
• curare la sicurezza on-line della comunità scolastica;
• garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i menbri della comunità scolastica;
• assicurare che il personale riceva una formazione adeguata per svolgere i ruoli di sicurezza on-line e per la formazione di altri colleghi;
• garantire che vi sia un sistema in grado di monitorare il personale di supporto che svolge le procedure di sicurezza online interne.
• Assicurare nei limiti delle risorse finanziarie disponibili l'intervento di tecnici per garantire che l'infrastruttura tecnologica della scuola sia funzionante, sicura, non aperta ad uso improprio o a dannosi attacchi esterni;
• Favorire il il funzionamento dei diversi canali di comunicazione all'interno della scuola e fra la scuola e le famiglie.

2. il dsga

• assicura, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;
• garantisce che sia tenuto un registro di incidenti di sicurezza online;
• coordina con le autorità locali e le agenzie competenti;
• controlla l'accesso a materiali illegali/inadeguati;
• controlla eventuali azioni di cyberbullismo.

3. Animatore digitale e team dell'innovazione	• Stimolano la formazione interna negli ambiti di sviluppo della scuola digitale e fornire consulenza e informazioni al personale in relazione ai rischi online ed alle misure di prevenzione e gestione degli stessi; • Monitorano e rilevano le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola; • Assicurano che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate; • Curano la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti; • Coinvolgono la comunità scolastica nella partecipazione ad attività e progetti attinenti la scuola digitale; • Inseriscono l'educazione all'uso consapevole delle TIC e alla sicurezza online all'interno del curricolo di studi; • Collaborano con il personale tecnico esterno in forza alla scuola. • promuovono l'aggiornamento dei docenti; • contribuiscono alla diffusione dell'innovazione nella scuola, a partire dai contenuti del Pnsd; • sviluppano progettualità sugli ambiti della formazione interna e sulla creazione di soluzioni innovative.

4. docente funzione strumentale per le nuove tecnologie	• cura il sito web della scuola per scopi istituzionali e consentiti; • supporta l'attività laboratoriale con consigli, aiuti e chiarimenti; • monitora l'utilizzo delle TIC e segnala al DSGA eventuali problemi che dovessero richiedere acquisti o interventi tecnici; • assicura che il personale possa accedere alla rete della scuola solo tramite password; • fornisce al personale, agli alunni e ai genitori consulenza e informazioni in relazione ai rischi on line e alle misure di prevenzione e gestione degli stessi; • riceve segnalazioni di incidenti e-Safety e crea un registro degli incidenti e informa il DS. Referente Cyberbullismo/Team Antibullismo deve/devono. • partecipare ai corsi di formazione per l'acquisizione di idonee competenze teoriche e pratiche; • Pubblicizzare attività formative per i docenti; • Favorire la conoscenza del fenomeno e gli strumenti di prevenzione dello stesso affinché le famiglie possano riconoscerlo ed intervenire in modo corretto; • Sostenere le famiglie e i minori vittime del cyberbullismo; • Promuovere, in collaborazione con tutti gli insegnanti, l'educazione all'uso consapevole della ret

5. docenti

• Eucano alla sicurezza online nello svolgimento della propria disciplina;
• Supervisionano e guidano gli alunni quando sono impegnati in attività di apprendimento che coinvolgono tecnologie online;
• Si assicurano che gli alunni siano capaci di ricercare contenuti online in sicurezza e siano pienamente consapevoli dei problemi relativi ai contenuti elettronici (come ad esempio le leggi sul copyright).
• danno chiare indicazioni sul corretto utilizzo della strumentazione multimediale, di internet, ecc.;
• segnalano prontamente eventuali malfunzionamenti o danneggiamenti al docente funzione strumentale;
• non divulgano le credenziali di accesso alla rete wifi;
• non salvano sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili;
• si informano/si aggiornano sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
• si assicurano che gli alunni seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;
• controllano l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
• nelle lezioni in cui è programmato l'utilizzo di Internet, guidano gli alunni a siti controllati e verificati come adatti per il loro uso e controllano che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
• segnalano al Dirigente Scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme e/o stabiliscono comuni linee di intervento educativo per affrontarle;

6. il personale ata

• deve prendere parte agli incontri formativi promossi dall'IISS "Don Michele Arena" sulle tematiche della privacy e della digitalizzazione;
• deve avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
• deve monitorare l'uso di dispositivi tecnologici e attuare politiche scolastiche per quanto riguarda questi dispositivi;
• deve segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o ai suoi collaboratori o alla Funzione Strumentale per le nuove tecnologie o all'Animatore Digitale per le opportune indagini / azioni / sanzioni;

7. gli studenti

• devono Leggere, capire e aderire alla e-Policy dell'Istituto;
• devono Adottare comportamenti rispettosi nella comunicazione in rete osservando la Netiquette dell'IISS "Don Michele Arena"
• devono utilizzare le TIC su indicazioni del docente;
• devono, in caso di riscontro di malfunzionamenti della strumentazione e/o di contatto accidentale con informazioni, immagini e/o applicazioni inappropriate, comunicarlo immediatamente all'insegnante;
• non devono eseguire tentativi di modifica della configurazione di sistema delle macchine;
• non devono utilizzare la strumentazione della scuola a scopi personali, ludici e/o ricreativi (a meno che l'attività didattica non lo preveda esplicitamente);
• non devono utilizzare propri dispositivi esterni personali senza aver acquisito il permesso da parte dell'insegnante;
• devono chiudere correttamente la propria sessione di lavoro;
• devono essere consapevoli dei problemi di sicurezza connessi con l'uso di telefoni cellulari, telecamere e dispositivi portatili;
• devono essere responsabili dell'utilizzo delle attrezzature tecnologiche della scuola e comprendere l'importanza di adottare buone pratiche di e-Safety anche quando utilizzano tecnologie digitali fuori dalla scuola.
• devono avere una buona comprensione delle capacità di ricerca e della necessità di evitare il plagio e rispettare normative sul diritto d'autore;
• devono conoscere e capire l'azione educative della scuola sull'uso improprio di immagini e il cyberbullismo.
• Non pubblicare mai, senza l'esplicito permesso dell'autore, il contenuto di messaggi di posta elettronica o privati.
• Non essere intolleranti con chi commette errori sintattici o grammaticali. Chi scrive è comunque tenuto a migliorare il proprio linguaggio in modo da risultare comprensibile alla collettività.

- 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).

I soggetti esterni che sono responsabili di iniziative educative e formative presso l'IISS "Don Michele Arena": prendono visione della politica dell'Istituto riguardo all'uso consapevole e responsabile della rete e delle TIC, promuovono la sicurezza on-line durante le attività di cui sono titolari, segnalano ai docenti preposti e al Dirigente Scolastico eventuali comportamenti problematici o casi di abuso nell'uso della rete e delle TIC.

Tutti gli attori, operatori o stakeholder, 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.

- 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.

Il presente documento sarà oggetto di disseminazione per l'intera comunità scolastica con il coinvolgimento di studenti, docenti e famiglie. La scuola si impegna a promuove eventi informativi e formativi, rivolti a tutto il personale, agli alunni e ai loro genitori, anche con il coinvolgimento di esperti.

Condivisione e comunicazione della Policy agli alunni:

- attraverso attività, laboratori, incontri, spettacoli che portino a riflettere sui rischi e opportunità del web.

Condivisione e comunicazione della Policy al personale:

- le norme adottate dalla scuola in materia di sicurezza nell'utilizzo del digitale saranno rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito web della scuola.

Condivisione e comunicazione della Policy ai genitori:

- le famiglie saranno informate in merito alla linea di condotta adottata dalla scuola per un uso sicuro e responsabile delle tecnologie digitali e di internet

attraverso la condivisione del presente documento e di materiali informativi specifici sul sito web della scuola.

Per tutto il personale sono previsti aggiornamenti e nuova formazione in materia di sicurezza online.

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.

- 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.

Il regolamento d'istituto, il regolamento di condotta,Il rgolamento ed il piano DDI dell'IISS "Don michele Arena" prevedono casistiche di infrazioni e corrispondenti sanzioni nel rispetto della gradualità e proporzionalità.

Tutte le infrazioni alla presente Policy andranno segnalate al Dirigente Scolastico, che valuterà le possibili azioni da intraprendere. Verranno prese tutte le precauzioni necessarie per garantire la sicurezza on-line.

Interventi sugli alunni:

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

- un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare (cyberbullismo);
- l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;
- la condivisione di immagini intime o troppo spinte;
- il collegamento a siti web non indicati dai docenti.

Gli interventi correttivi previsti per gli alunni sono riferiti all'età e al livello di sviluppo cognitivo degli alunni. Sono previsti, quindi, provvedimenti disciplinari proporzionati all'età e alla gravità del comportamento, quali:

- il richiamo verbale;
- il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività);

- il richiamo scritto con annotazione sul diario;
- il ritiro del cellulare fino a fine giornata;
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente scolastico;
- la rimozione da internet o del computer di accesso per un periodo;
- comunicazioni alle autorità competenti;

Le denunce di bullismo online saranno trattate in conformità con la legge attuale (L.71/2017).

Sono anche previsti interventi di carattere educativo, di rinforzo dei comportamenti, correttivi e riparativi dei disagi causati, di promozione della conoscenza e della gestione delle emozioni, di prevenzione e gestione positiva dei conflitti, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di promozione di rapporti amicali e di reti di solidarietà, di moderazione dell'eccessiva competitività.

Interventi sul personale scolastico:

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

- una carente istruzione preventiva degli alunni sull'utilizzo corretto e responsabile delle tecnologie digitali e di internet;
- un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- 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 l'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 vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.

Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge.

Interventi sui genitori:

Alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche verificatisi al di fuori del contesto scolastico. I genitori degli alunni possono essere convocati per concordare misure educative diverse, provvedimenti disciplinari oppure essere sanzionati a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri; giova ricordare a tal proposito l'impegno manifestato dalla famiglia sottoscrivendo il patto di corresponsabilità, ed eventuale culpa in educando.

- 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.

La e-safety policy fa riferimento e si armonizza con tutti gli altri regolamenti vigenti nell'Istituto, in particolare con Regolamento d'Istituto, Regolamento e Piano DDI;

Integra tali regolamenti costituendo la sezione relativa all'uso delle nuove tecnologie, dei nuovi ambienti di apprendimento e delle metodologie didattiche offerti dall'Istituto (scuola 2.0, etc.).

Tutto ciò che qui non è normato è da considerarsi regolamentato secondo la disciplina generale.

Riassumendo: il presente documento si integra con gli obiettivi e i contenuti dei seguenti documenti:

- PTOF;
- Regolamento d'Istituto Sezione - Prevenzione e Contrasto del "Bullismo e Cyberbullismo",
- Patto Educativo di corresponsabilità.

- Regolamento e Piano DDI

- 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 verrà curato dal DS in collaborazione con le Funzioni Strumentali, l'Animatore Digitale e il Team dell'Innovazione che promuoveranno inoltre gli eventuali aggiornamenti che si rendano opportuni, secondo una logica di condivisione con tutto il corpo docente e le famiglie

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

1. Organizzare almeno un evento di presentazione del progetto Generazioni Connesse rivolto ai docenti;

2. Organizzare almeno un evento congiunto di presentazione del progetto generazioni connesse e di altri progetti/UDA sulla problematica del bullismo/cyberbullismo agli studenti e ai genitori

3.Partecipare al Safer Internet Day 2024, la Giornata Mondiale dedicata all'uso positivo di Internet;
Azioni da svolgere nei prossimi 3 anni:

1.Organizzare laboratori didattici per l'approfondimento delle tematiche/problematiche riconducibili al bullismo e al cyberbullismo stimolando gli studenti a realizzare dei prodotti finali con l'utilizzo di UDA dedicate;

2. Incontrare le famiglie, anche in modalità telematica nel dominio @iissarena.edu.it, per favorire l'alleanza con la scuola al fine di sviluppare strategie di prevenzione e d'intervento;
3. Utilizzo di una email istituzionale accessibile solo al Dirigente Scolastico e al Referente per mantenere la privacy di chi vuole informare/denunciare casi di bullismo/cyber bullismo di cui si è vittima o di cui si è a conoscenza.

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.

Aree di competenza

informazione comunicazione

creazione di contenuti problem-solving sicurezza Descrittori di competenza

Lo studente identifica, localizza, recupera, conserva le informazioni digitali secondo un approccio "intuitivo" Lo studente identifica, localizza, recupera le informazioni digitali con consapevolezza e con atteggiamento critico; conserva, organizza e analizza le informazioni digitali

Lo studente comunica in ambienti digitali, condivide risorse attraverso strumenti on-line, sa collegarsi con gli altri e collabora attraverso strumenti digitali, interagisce e partecipa alle comunità e alle reti .

Lo studente realizza e modifica contenuti (da elaborazione testi a immagini e video); integra e rielabora conoscenze, produce contenuti in modo creativo Lo studente utilizza gli strumenti digitali per identificare e risolvere piccoli problemi tecnici, contribuisce alla creazione di conoscenza, produce risultati creativi ed innovativi, supporta gli altri nell'uso degli strumenti digitali

Lo studente riflette e acquisisce consapevolezza su protezione personale, protezione dei dati, protezione dell'identità digitale, misure di sicurezza; conosce ed applica i diritti di proprietà intellettuale e le licenze.

Strumenti Rete e connettività

Registro elettronico e ambiente di lavoro condiviso Google Workspace (Gmail, Google Drive, Google Documenti, ...) come ambiente informatico ad accesso gratuito per la gestione e condivisione di materiale didattico, corsi, verifiche formative e sommative, prove comuni, consegne

Video didattici in rete (es. YouTube, risorse digitali dei manuali in adozione, RAI Scuola, RAI Play) Software per la produzione di documenti, fogli di calcolo e presentazioni, Software per lo sviluppo del pensiero computazionale e il making educativo, Software per la realizzazione di mappe concettuali e video tutorial (es. Premiere, Windows media player, Powtoon) Software per videoconferenza (Zoom, Skype, Teams, Chat GPT4, Board, Copilot...).

Traguardi formativi

Utilizzare la rete per scopi di informazione, comunicazione, ricerca e svago Utilizzare strumenti informatici e di comunicazione per elaborare dati, testi e immagini e produrre documenti Conoscere le caratteristiche e le potenzialità tecnologiche degli strumenti d'uso più comuni (PC, tablet, smartphone, strumenti archiviazione memoria digitale) Riconoscere vantaggi, potenzialità, limiti e rischi connessi all'uso delle tecnologie più comuni, anche informatiche Apprendere a utilizzare gli "aggregatori" digitali Cogliere e sfruttare le potenzialità creative e non solo quelle funzionali delle applicazioni digitali Apprendere a discriminare le fonti di informazione più affidabili

La competenza digitale, per la sua importanza nelle attività professionali e anche quotidiane, è ritenuta dall'Unione Europea una competenza chiave per lo sviluppo del senso di cittadinanza. Nel curricolo disciplinare del nostro Istituto tale competenza pervade in modo trasversale i vari insegnamenti; questa declinazione scaturisce dalla necessità di dare almeno una formazione di base sull'uso delle TIC, inserendole nelle attività didattiche, per fornire gli strumenti per un approccio consapevole, critico, autonomo e responsabile. Tali competenze sono oggetto di certificazione, come da apposito documento ministeriale, al termine della scuola Secondaria. Negli ultimi anni la scuola ha provveduto all'implementazione della dotazione digitale dei vari plessi,

anche attraverso la partecipazione ai progetti PON, per consentire l'introduzione di metodologie basate sull'uso delle TIC.

Presso l'IISS "Don Michele Arena" sono stati attivati percorsi di Educazione alla cittadinanza digitale, costruendo itinerari di approfondimento e di sviluppo di materiale informativo sul diritto alla connessione come diritto fondamentale dell'uomo, e sul rispetto e sui limiti della libertà di espressione on-line. Tali tematiche sono riconducibili all'insegnamento di Educazione Civica.

Il Curricolo Di Educazione Civica

In ottemperanza alle disposizioni della L92/2019 e del DM35/2020 con annesse linee guida, l'IISS "Don Michele Arena" ha integrato il curricolo d'Istituto progettando almeno 33 ore da dedicare all'insegnamento dell'Educazione Civica, che tra i nuclei fondanti tratta di cultura della legalità e di Educazione Digitale. Il curricolo verticale per classi parallele sviluppa in modo trasversale le competenze riferite al Pecup in materia di Educazione digitale, tutela della privacy, ed esercizio dei principi della cittadinanza digitale con competenza e coerenza rispetto al sistema integrato di valori cheregolano la vita democratica.

- 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.

I docenti, in conformità con quanto previsto dal piano triennale dell'offerta formativa, hanno partecipato a corsi di formazione nell'ambito di piani nazionali e ad iniziative organizzate dall'istituzione o dalle scuole associate in rete incrementando le competenze digitali di base. I docenti del team digitale hanno seguito la formazione ad essi destinata, che a cascata risulta spendibile all'interno dell'Istituto. Nel corso del

corrente anno il team digitale intende promuovere iniziative di autoformazione interna gestita da docenti dell'istituto; i docenti potranno avvalersi altresì dei corsi di aggiornamento promossi dall'Ambito Territoriale oppure presenti sulla piattaforma ELISA e SOFIA riguardanti l'innovazione didattica e la didattica digitale. Il piano di formazione annuale per i docenti e per il personale non docente dell'IISS "Don Michele Arena" presta particolare attenzione alla tematica della digitalizzazione e dell'uso consapevole della rete avendo deliberato un corso di formazione rivolto agli studenti sulla sicurezza in rete e uso consapevole di internet e delle nuove tecnologie. Contenuti dell'intervento formativo programmato per l'a.s. 2023/2024: adescamento online-cyberbullismo – contenuti inadatti – sexting – Il galateo online - dipendenza online-rendere Internet un luogo più sicuro per gli utenti più giovani promuovendone un uso positivo e consapevole.

- 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.

La formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet può prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi.

L'IISS "Don Michele Arena" promuove e progetta la formazione dei docenti sulle tematiche dell'inclusione, dell'uso consapevole delle TIC (uso della Lim, uso del Registro Elettronico, piattaforma g.suite di google, programmi e applicazioni per la creazione di mappe).

Diversi incontri sono stati organizzati in collaborazione con la Polizia di Stato, la Guardia di Finanza, i Carabinieri sulla sicurezza in rete, reati connessi al cyberbullismo, furto d'identità e frodi online.

- 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.

L'IISS "don Michele Arena" garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'e-Policy 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.

L'Istituto ha promosso e continua a promuovere iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine sono previsti incontri fra genitori e specialisti (docenti, forze dell'ordine) per la diffusione del materiale informativo su queste tematiche. Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo. Sul sito scolastico e sulla relativa bacheca virtuale relativa a "Generazioni connesse" saranno messi in condivisione materiali dedicati ad alunni e alle famiglie come guide in formato pdf e video che possono fornire spunti di approfondimento e confronto. La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento (Policy e-safety) per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e prevenire i rischi legati a un utilizzo non corretto di internet.

Il nostro piano d'azioni

AZIONI da sviluppare nell'arco del triennio 2024/2027

1. Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica in coerenza con il piano di formazione deliberato in Collegio Docenti;
2. Organizzare incontri con esperti per i docenti sulle competenze digitali.
3. Inserire e diffondere materiale utile alle famiglie per prevenire e contrastare fenomeni devianti

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

1. Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
2. Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
3. Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
4. Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
5. Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
6. Organizzare incontri con esperti per i docenti sulle competenze digitali.
7. Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

- 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.

In questo spazio dell'ePolicy dedichiamo attenzione 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.

In ottemperanza a quanto previsto dal Regolamento Generale sulla Protezione dei Dati, (UE) 679/2016 "GDPR" con effetti diretti a partire dal 25 maggio 2018, recepito in Italia col decreto legislativo n.101 del 10-08-2018, vigente dal 19 settembre 2018, che inserisce la figura obbligatoria nella P.A. del Responsabile della Protezione dei Dati (RPD), l'IISS "Don Michele Arena" si avvale della consulenza di esperti nele settore della tutela della privacy avendo individuato il proprio RPD nel rappresentante della Idnet management.

In apposita sezione del sito web istituzionale sono pubblicati i modelli di liberatoria da utilizzare, conformi alla normativa vigente in materia di protezione dei dati e le informative agli operatori della scuola e alle famiglie.

L'infrastruttura e la strumentazione ICT dell'Istituto sono un patrimonio di tutti, esse vanno utilizzate nel rispetto delle norme contenute nel Regolamento d'Istituto e nel DVR.

Nello specifico si possono individuare alcune linee guida di e-safety:

- Si consiglia al personale scolastico di non condividere i propri contatti telefonici e e-mail personali, salvo in occasione di particolari eventi (es. viaggi di istruzione). Si caldeggia, invece, l'utilizzo dei contatti ufficiali della scuola.
- All'atto dell'iscrizione sarà richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso di immagini e video delle/dei minori per finalità strettamente connesse alla vita scolastica.
- Le fotografie o i video da pubblicare sul sito che includano allieve e allievi saranno selezionati tenendo conto dei consensi espressi dai genitori ad inizio anno scolastico.

L'accesso ad infrastrutture e strumentazione ICT utilizzabili per la didattica è riservato agli insegnanti, agli alunni è limitato al perseguimento di scopi formativi. I docenti devono formare i propri alunni al rispetto del suddetto Regolamento, per gli aspetti di loro pertinenza.

L'Istituto è dotato di una rete wireless nei 4 plessi e l'accesso ad internet è consentito a scopi didattici al personale docente attraverso l'assegnazione di una password

comune a tutti. Agli alunni è permessa la navigazione in internet dai pc del laboratorio o delle aule collegate alle LIM sotto il diretto controllo dei docenti e dei tecnici di laboratorio.

- 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'IISS "Don Michele Arena" utilizza un piano di revisione del sistema di filtraggio presente nei vari plessi, così da evitare il più possibile l'accesso a siti inappropriati al contesto scolastico. Sono scelti software antivirus considerati dal personale tecnico più efficaci. Ai tecnici di laboratorio e all'amministratore di sistema si affida il compito di mantenere costantemente aggiornati i suddetti software. Tutti i plessi dell'Istituto sono dotati di una rete wireless alla quale sono connessi la maggior parte dei devices. Recentemente si è provveduto al cablaggio di 2 plessi al fine di potenziare la connettività, anche in risposta alla sfida della DDI e della DAD in base all'andamento epidemiologico.

I dispositivi sono collegabili alla rete internet esclusivamente tramite password. Si ritiene utile che il personale docente di ogni plesso, o almeno un rappresentante di essi, sia a conoscenza della password di accesso, così da poter connettere facilmente tutti i dispositivi necessari per lo svolgimento delle attività didattiche. Nell'ottica di un maggior sviluppo del "Byod" (ossia l'utilizzo di dispositivi elettronici personali durante le attività didattiche), si ritiene propositivo l'utilizzo dei dispositivi a fini didattici e la scuola rende fruibili altresì tablet per lo svolgimento di verifiche e ricerche online.

- 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.

L'IISS "Don Michele Arena" dispone di indirizzo di posta elettronica istituzionale e pec. Gli indirizzi e i contatti utili sono pubblicati sul sito di istituto, cosicché si possa conoscere con immediatezza l'indirizzo del destinatario desiderato. Il personale interno alla scuola (D.S., docenti, personale di segreteria) e i genitori hanno a disposizione la piattaforma di registro elettronico "ARGO" per comunicazioni "interne". l'Istituto ha chiesto l'iscrizione alla piattaforma Google Workspace, che consente l'utilizzo di molte applicazioni utili alla didattica, all'organizzazione delle attività in classe e alle comunicazioni tra utenti.

Sulla piattaforma possono operare sia i docenti che gli studenti a cui è stato attribuito un proprio account nel dominio @iissarena.edu.it

Sito web della scuola

Il sito web della scuola (www.iissarena.edu.it) è la prima e principale interfaccia dell'Istituto. Oltre alle informazioni generali e di contatto, vi si trovano apposite sezioni dedicate a docenti, personale ATA e famiglie degli alunni con informazioni, circolari, modulistica, presentazione di attività e progetti.

Social network

L'Istituto al momento, non ritiene necessario attuare azioni in questa direzione. E' severamente vietato agli studenti e a tutto il personale della scuola la pubblicazione sui social network di immagini e/o video realizzati nel contesto scolastico che possano ledere la privacy dei soggetti coinvolti e per i quali non sia stata acquisita apposita liberatoria.

- 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.

Strumentazione personale Per gli studenti

Durante le attività didattiche gli studenti sono autorizzati ad utilizzare la strumentazione personale quali cellulari, tablet ecc. solo ed esclusivamente per uso didattico e sotto il controllo del docente; agli studenti non è permesso utilizzare i telefoni cellulari per telefonare, scattare foto, registrare filmati durante le lezioni o durante l'orario scolastico. È vietato inviare messaggi illeciti o inappropriati, nonché fotografie o filmati. La connessione ai servizi di internet per la propria strumentazione viene fatta su rete personale. Eccezione sono gli alunni con BES o DSA, per i quali la scuola garantisce il supporto tecnologico idoneo, ma su richiesta: a loro è consentito l'uso della strumentazione personale con l'accesso alla rete wifi dell'istituto.

Per i docenti Durante le ore delle lezioni non è consentito l'utilizzo del cellulare se non per finalità strettamente didattica. È consentito l'uso di altri dispositivi elettronici personali sempre solo a scopo didattico ed integrativo di quelli scolastici disponibili. Durante il restante orario di servizio è permesso l'uso di portatili, tablet, per attività funzionali all'insegnamento in entrambe le situazioni ed è garantito l'accesso alla rete wifi negli spazi comuni previsti dalla logistica della rete stessa. Per il personale della scuola Durante l'orario di servizio al personale scolastico è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente.

Il nostro piano d'azioni

AZIONI (da sviluppare nel triennio 2024/2027).

1. 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
2. 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);
3. Partecipare a concorsi nazionali e locali stimolando gli studenti a produrre video-spot-fumetti-slogan che facciano sviluppare la percezione e il riconoscimento oggettivo del fenomeno del bullismo e del cyberbullismo.
4. Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
5. Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
6. Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da

parte del personale Tecnico Amministrativo e dagli ATA

7. 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
8. 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
9. Implementare lo spazio dedicato sulla homepage del sito web istituzionale.

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

- 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.*

«Smartphone e Internet hanno rivoluzionato l'accesso dei giovani all'informazione, ma un sondaggio rileva quanto attraverso il web sia reale il rischio di abusi per ragazzi e ragazze», sottolinea Cornelius Williams, Direttore associato dell'UNICEF per i programmi di protezione dell'infanzia

.Il rapporto mostra che la larga maggioranza degli adolescenti manifesta confidenza nelle proprie abilità di navigare in modo sicuro: circa il 90% degli intervistati ritiene di sapere evitare i pericoli online.

Di fronte a minacce sul web, la maggior parte degli adolescenti si rivolge agli amici più che a genitori o insegnanti. Tuttavia, meno della metà dei ragazzi intervistati ha affermato che saprebbe aiutare un amico ad affrontare un pericolo online.

Interventi di sensibilizzazione

Si parla spesso di interventi o campagne di sensibilizzazione, si tratta in questi casi di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento.

Molte campagne di sensibilizzazione hanno, ad esempio, una risonanza internazionale che può mirare a:

- mettere in luce una determinata problematica o condizione,
- chiedere ad una determinata utenza di attivarsi per una causa,
- raccogliere dei fondi.
- Altri interventi possono, invece, essere mirati a piccoli gruppi o comunità (come ad esempio la comunità scolastica), con l'obiettivo di coinvolgere un gruppo ristretto di persone affinché agiscano insieme in favore di una causa in cui credono.

- 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).

È possibile suddividere gli atti di cyberbullismo in due grandi gruppi:

1. cyberbullismo diretto: il bullo utilizza strumenti di messaggistica istantanea (es. sms, mms) che hanno un effetto immediato sulla vittima, poiché diretti esclusivamente a lei.
2. cyberbullismo indiretto: il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima anche da un punto di vista psicologico.

È molto importante sottolineare come il cyberbullismo non sia una problematica che riguarda unicamente vittima e cyberbullo. È un fenomeno sociale e di gruppo. Infatti, centrale è il ruolo delle agenzie educative e di socializzazione (formali e informali) più importanti per gli adolescenti: la famiglia, la scuola, i media, le tecnologie digitali e il gruppo dei pari.

- 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.

Il web è sempre più spesso il palcoscenico sul quale i cd. 'leoni da tastiera' amano esibirsi diffondendo odio ed arrecando lesione al decoro ed alla reputazione altrui. I commenti basati sulla discriminazione si susseguono incessantemente in questo periodo, gettando la vittima in pasto alla gogna mediatica, con gravi ripercussioni sul benessere psicofisico delle vittime.
Ma vediamo da vicino chi sono gli haters e cosa si intende per incitamento all'odio, nonché le conseguenze per chi si rende protagonista di tali vicende.

Chi sono gli haters?

Gli haters, ovvero 'odiatori', sono coloro che sul web, ed in particolare sui social, si rendono autori di atti di odio, disprezzo e critiche nei confronti di personaggi famosi o comunque posti sotto i riflettori dei mass media per fatti di cronaca che hanno colpito l'opinione pubblica.

Riversare rabbia e odio sugli altri attraverso il web crea negli haters un distacco dalla realtà, fornendo loro l'illusione dell'impunità, come se ciò che si scrive nel web fosse 'irreale'. Lo scudo della tastiera e la percezione dei social come 'piazza virtuale' dove tutto è concesso, dove regnerebbe sovrana l'anarchia, deresponsabilizzano l'autore delle condotte d'odio, attenuando ai suoi occhi la gravità delle stesse. Nulla di più falso!

Le condotte criminose perpetrate sul web, infatti, vengono punite alla legge italiana

che, nel corso degli ultimi anni, ha dovuto tener conto dell'avvento dei social per prevedere nuove ipotesi di reato o anche per applicare aggravanti a reati perpetrati sul web. Gli haters, infatti, si rendono responsabili di diversi reati: diffamazione aggravata, molestie, cyberstalking fino ad arrivare all'incitamento all'odio.

L'impatto o l'impatto potenziale

L'impatto reale o potenziale esercitato sugli individui, sui gruppi o sull'insieme della società è una delle principali considerazioni da tenere presenti. Spesso, le ripercussioni negative subite dall'individuo o dal gruppo si rivelano più importanti della valutazione dell'episodio da parte di osservatori esterni.

Come intervenire?

Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono quindi un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete.

Occorre in tal senso 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.

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

l'IISS "Don Michele Arena"intende concretizzare le seguenti azioni in merito alla problematica:

- partecipazione ad incontri con la Polizia Postale e la Polizia di Stato;
- per le classi del biennio laboratori e prodotti finali riconducibili alle unità di apprendimento sulla prevenzione del bullismo e del cyberbullismo;
- collaborazione con l'Arma dei Carabinieri per le classi quinte in tema di prevenzione e sensibilizzazione sui reati legati all'utilizzo di internet e delle piattaforme on-line;
- presenza a scuola di referente dello Sportello d'ascolto, attività dello Sportello d'ascolto in presenza e/o online-servizio di consulenza degli esperti dell'IstitutoWalden;
- iniziative, progetti e attività di PCTO mirati all'inclusione, all'accettazione e alla valorizzazione della diversità, al dialogo interreligioso e interculturale, alla destrutturazione degli stereoitipi, alla prevenzione della violenza di genere.

- 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'IISS "Don Michele Arena" da sempre sensibile alla tematica/problematica ha negli anni proposto e continua a promuovere azioni di prevenzione attraverso:

- incontri con il SERT;
- testimonianze dirette di giovani che hanno vinto la dipendenza da internet e di giovani e adulti che sono riusciti a staccarsi dal mondo dei giochi online;
- supporto psicologico e guida da parte dei professionisti dello sportello ascolto;
- progetto PTOF dipendenze da alcol, droga e nuove forme di dipendenze (giochi d'azzardo online, nomofobia);
- trattazione della tematica nelle UDA del nuovo insegnamento di Educazione Civica;
- presenza nell'organigramma d'Istituto della referente alla salute.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.

- 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.

È importante essere consapevoli delle conseguenze che il sexting può avere. Le

immagini di nudo o sessualizzate non sono contenuti neutri, per questo è importante parlare delle possibili conseguenze legate a produzione, invio e condivisione di immagini di nudo.
Vediamo quali possono essere alcune delle principali conseguenze del sexting:

- Le conseguenze del web.
  Quando si perde il controllo delle immagini prodotte, la loro diffusione su web e social network è difficilmente gestibile. È bene precisare che in questo caso non si parla più di sexting ma di "revenge porn" (quando le immagini vengono ad esempio utilizzate da un/a ex partner a scopi vendicativi e con l'obiettivo di ledere la reputazione della persona ritratta), o di "sextortion" e cyberbullismo (cioè la minaccia di diffusione del materiale foto/video, sempre con l'obiettivo di ledere la reputazione della persone ritratta).
- Conseguenze legali.
  Anche quando non c'è intenzione di danneggiare l'altra persone né di commettere un abuso online (come nei casi del revenge porn o della sextortion), non è escluso che i comportamenti tipici del sexting possano configurare reati connessi con la pedopornografia. Secondo il nostro ordinamento il materiale scambiato in forma di sexting si declina come pedopornografico, quando se ne perde il controllo, anche ingenuamente. Secondo il recente parere emesso del Comitato di Lanzarote del Consiglio d'Europa (l'organismo che monitora l'attuazione della Convenzione del Consiglio d'Europa sulla protezione dei bambini contro lo sfruttamento e gli abusi sessuali), il "sexting" tra minori non costituisce una condotta connessa alla "pedopornografia", se destinato esclusivamente all'uso privato dei minori. Il parere specifica però che i minori costretti a tale condotta dovrebbero essere affidati ai servizi di assistenza alle vittime e non essere perseguiti penalmente.
- Conseguenze emotive.
  Queste riguardano l'affettività e in particolare il tema del consenso. La pressione dei pari ("lo fanno tutti o tutte"), ricatti o minacce ("se non lo fai, non mi ami"), problemi di autostima o il sentirsi in dovere nei confronti del proprio partner al fine di evitare il senso di colpa, possono essere tutti elementi che portano un ragazzo o una ragazza a cedere a comportamenti che non rispettano i suoi tempi o desideri. Per questo motivo, è importante che il ragazzo o la ragazza sia equipaggiato/a con strumenti che gli/le consentano di leggere criticamente quello che vede o sperimenta, anche quando si tratta della sua sessualità, per poter, ad esempio, definire i propri confini e riconoscere quando una richiesta esterna li supera. I ragazzi e le ragazze hanno il diritto di vivere la sessualità secondo tempi e modi adatti alla loro maturità e questo può avvenire solo se possono contare su conoscenze e competenze specifiche, in grado di orientarli e guidarli nelle loro scelte anche online. L'educazione alla sessualità all'affettività è fondamentale, per prevenire forme di abuso e per permettere ai minoridi effettuare scelte che migliorino la qualità della loro vita.

Il distacco sociale e l'isolamento, in generale, ma in particolare ora -determinati dalle

disposizioni per arginare la diffusione del Coronavirus - comportano difficoltà per tutte le relazioni, anche quelle dei più giovani, indipendentemente dal fatto di avere già una relazione affettiva anche prima dell'emergenza coronavirus, quindi il fenomeno del sexting sembra si stia pericolosamente diffondendo in questo periodo.

L'IISS "Don Michele Arena" organizza frequenti incontri con l'Arma dei carabinieri e con psicologi/assistenti sociali al fine di sensibilizzare i giovani e renderli consapevoli della gravità delle azioni e delle conseguenze anche di carattere penali.

- 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.

Se consideriamo quanto lo spazio della rete possa moltiplicare le occasioni e amplificare la portata dei mezzi in mano a coloro che esercitano comportamenti sopraffattòri, è sufficiente mettere insieme sexting e cyberbullying o grooming e snapchat,cioè combinare strumenti di per sé neutri con atteggiamenti negativi per averne un'idea. Se riflettiamo sull'esposizione personale implicata dalla rete per chi non è in grado di tutelarsi e sullo schermo offerto nel contempo a chi invece voglia approfittarne, comprendiamo facilmente la necessità di capire le parole con cui sono formulati i messaggi che sulla

rete corrono.

In inglese il sostantivo groom indicava in origine 'un ragazzo', successivamente 'un uomo di posizione inferiore; un domestico, un servitore' e, in particolare, 'l'addetto alla cura dei cavalli'; nell'inglese attuale sopravvive in quest'ultimo significato e in quello di 'sposo' nell'espressione bride and groom. Il verbo to groom significa "To tend as a groom; to curry, feed, and generally attend to (a horse); to 'fettle'" ['comportarsi come un groom, prendersi cura, e in generale occuparsi (di un cavallo)'; 'pulire, liberare dalle imperfezioni, rendere pulito']. A partire dall'inizio del secolo scorso il derivato grooming è usato nell'ambito dell'etologia in riferimento a un comportamento animale di pulizia reciproca, osservabile soprattutto negli uccelli e nei primati; soltanto alla fine del secolo è il termine passato a indicare, "Of a paedophile: to befriend or influence (a child), now esp. via the Internet, in preparation for future sexual abuse" ['di un pedofilo: avvicinarsi amichevolmente e cercare di influenzare (un bambino), adesso specialmente in rete, allo scopo di abusarne sessualmente'].

- 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.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024).

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

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

- 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.
- Organizzare uno o più incontri di formazione all'utilizzo sicuro e

consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.
- Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.
- Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella 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.

- 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.

- 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.

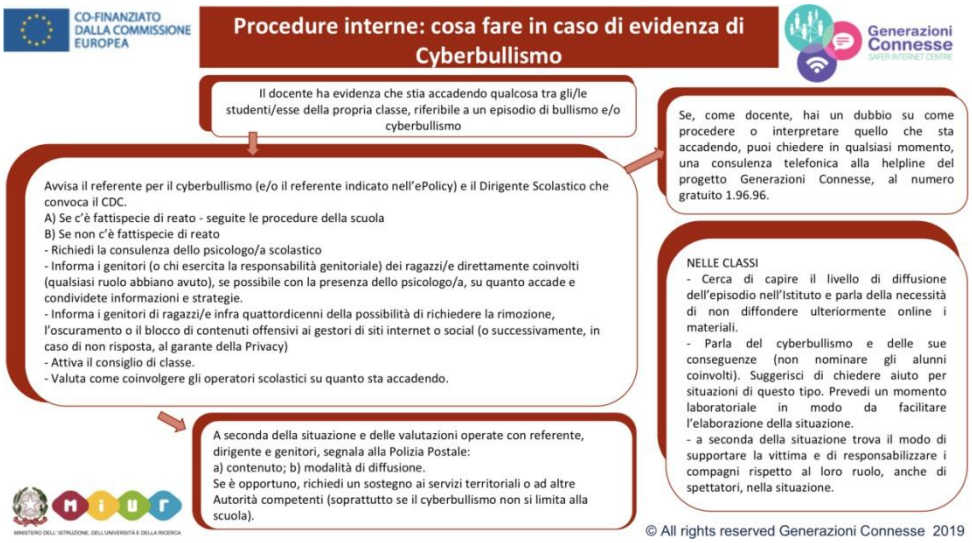
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **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.

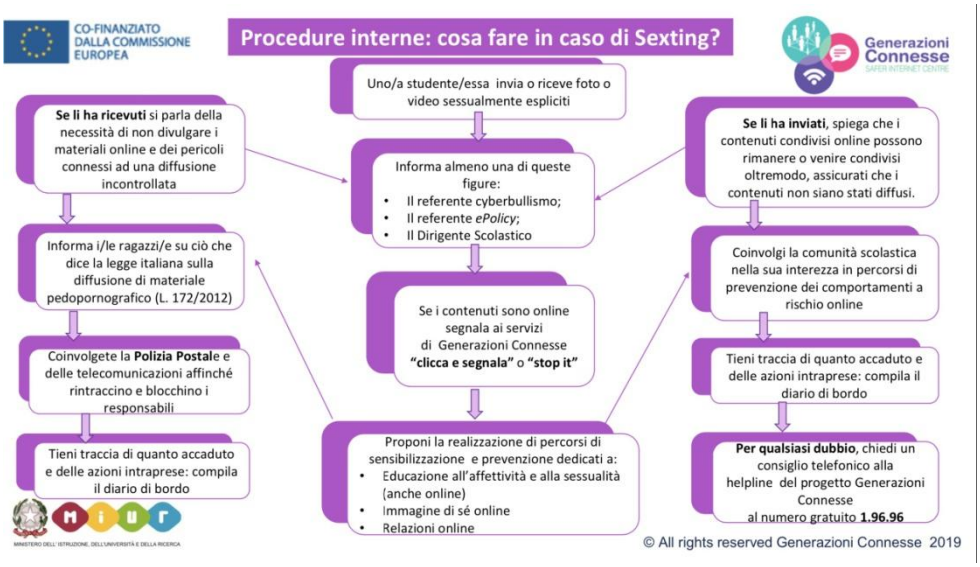
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

- *Allegati con le procedure*

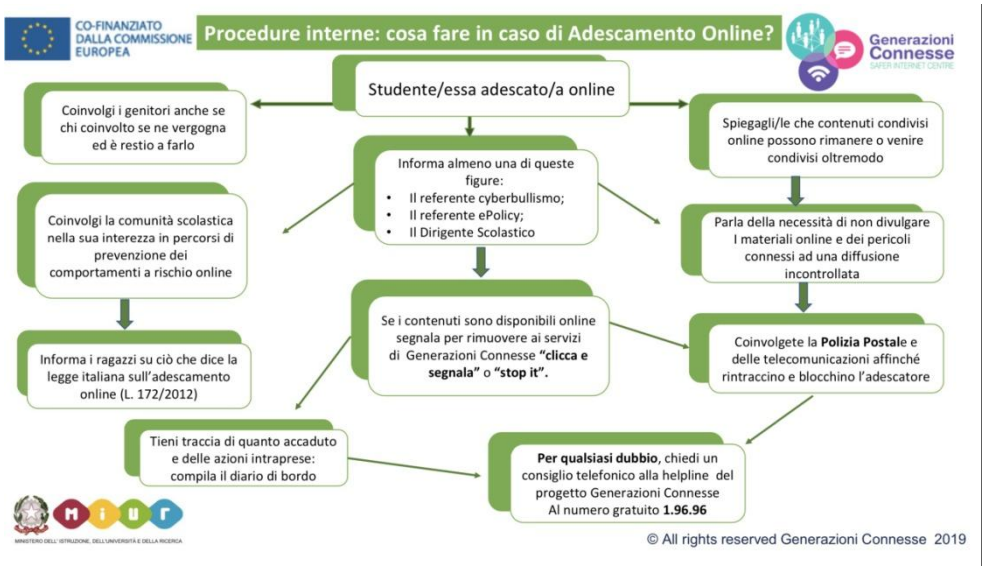
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



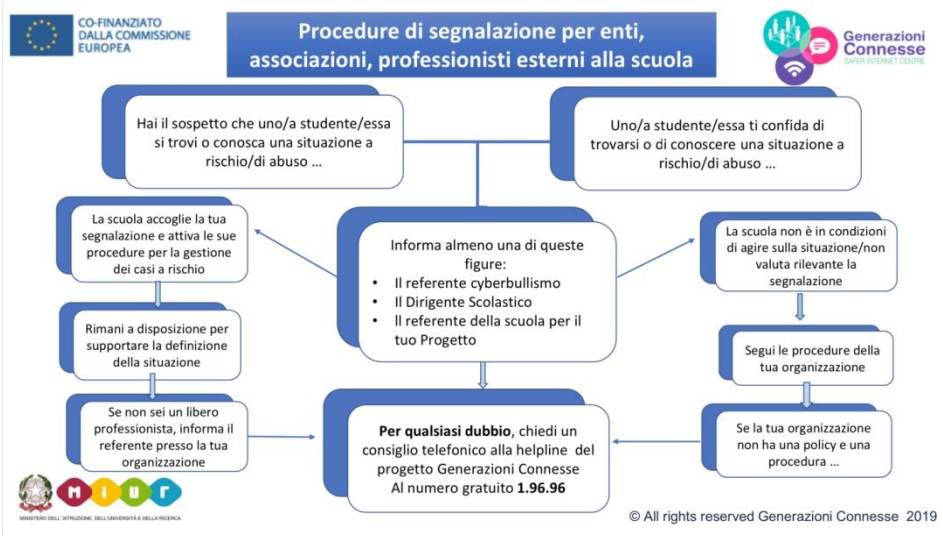
Procedure interne: cosa fare in caso di sexting?



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

Il nostro piano d'azioni

IL PIANO D'AZIONI dell'IISS "Don Michele Arena"

1. Trattazione delle tematiche sopra indicate nell'ambito di seminari/incontri con le forze dell'ordine e nelle UDA di Educazione Civica aree tematiche contrasto all'illegalità ed educazione digitale;
2. Formazione del personale docente, degli studenti e dei genitori;
3. Adesione a reti territoriali di scopo;
4. Favorire un clima di partecipazione collaborativa tra tutti soggetti presenti sul territorio a vario titolo coinvolti nella prevenzione del disagio giovanile, i CTS saranno informati delle situazioni di bullismo e cyberbullismo da parte delle scuole del territorio;
5. Implementazione del sito web istituzionale per la condivisione di link e materiali per il contrasto dei comportamenti devianti online;
6. Rafforzamento del patto di corresponsabilità già integrato in coerenza con la L92/2019 e con la normativa di riferimento per la DDI e condivisione con i genitori di materiali utili tratti anche da https://www.generazioniconnesse.it;

7. diffusione scheda di segnalazione atti di bullismo e cyberbullismo in sito web istituzionale e in classroom;
8. diario di bodo delle attività;
9. diffusione elenco reati procedibili d'ufficio;
10. -condivisione i.gloss@1.0 dei comportamenti devianti
11. Ulteriori azioni già descritte in piano d'azioni annuale e triennale delle diverse sezioni.