Documento di ePolicy

VAIS00400R

IS VALCERESIO

VIA ROMA 57 - 21050 - BISUSCHIO - VARESE (VA)

MARIA CARMEL SFERLAZZA

AGGIORNAMENTO A.S. 2024/2025 -------- TRIENNIO 2024/2027

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

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'uso delle tecnologie dell'informazione e della comunicazione (T.I.C.) è prassi quotidiana: gli studenti, le studentesse e l'intero corpo educante utilizzano questo strumento ogni giorno e non solo per attività connesse alla didattica. È fondamentale approcciarsi a queste tecnologie in modo consapevole e positivo.

L'e-policy vuole essere un documento volto a strutturare un intervento di sensibilizzazione, formazione e tutela di tutti gli utenti: ragazzi, ragazze e corpo educante.

È fondamentale acquisire dimestichezza e consapevolezza nell'uso delle T.I.C.:

queste, se utilizzate in maniera positiva, si rivelano uno strumento essenziale

- per la condivisione di informazioni, di elaborati e di contenuti;
- per documentare, condividere e organizzare attività didattica, risorse ed esperienze;
- per ricercare, selezionare e strutturare contenuti;
- per una comunicazione immediata e sicura;
- per una didattica che sia inclusiva e modulata sulle esigenze delle classi e sulle peculiari modalità di apprendimento di studenti e studentesse;
- per la formulazione di contenuti innovativi, attivi e modulati secondo diversi codici di comunicazione;
- per la gestione e l'organizzazione generale della scuola;

se utilizzate con poca consapevolezza, invece, possono portare a conseguenze dannose per la vita psicologica, fisica e relazionale di tutti 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.

Attraverso la stesura e la condivisione di questo documento autoprogrammato l'ISIS "Valceresio" definisce

- Le modalità attraverso le quali affronterà e proporrà un percorso di consapevolizzazione e formazione nell'uso delle TIC e dei dispositivi di accesso alle stesse
- Le norme e le procedure che assicurano un utilizzo responsabile e sicuro delle TIC
- Le strategie attraverso le quali monitorerà funzionalità, pertinenza e coerenza degli interventi formativi e delle attività proposte

- Le proposte per una prevenzione attiva ed efficace alle eventuali conseguenze connesse ad un uso scorretto delle TIC
- Le strategie di intervento per affrontare l'insorgenza eventuali problematiche derivate da un utilizzo poco consapevole di queste tecnologie

Attraverso la stesura di un'E-Safety Policy che traccia le linee guida per un uso sicuro delle nuove tecnologie, l'ISIS "Valceresio" si pone come obiettivo quello di promuovere l'acquisizione della consapevolezza dell'uso legittimo della rete, per far sì che internet possa solo avvantaggiare i giovani, il nostro Istituto aderisce al progetto "Generazioni Connesse".

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 @isisbisuschio.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'ISIS "Valceresio"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.

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'ISIS "Valceresio", 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.

6. 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'ISIS "Valceresio" 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, volte a rendere gli studenti protagonisti e attori attivi nelle attività di formazione, 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.

- organizzare incontri in presenza o a distanza con l'Associazione Nazionale Carabinieri (A.N.C.), con l'associazione generAzioni consapevoli, con la Polizia Postale e con esperti del settore, per coinvolgere gli studenti e studentesse attraverso testimonianze attive e aderenti alla realtà.

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.

1.2 - Ruoli e responsabilità

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

R U O L I

RESPONSABILITA'

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 membri 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 funzionamento dei diversi canali di comunicazione all'interno della scuola e fra la scuola e le famiglie.

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.

ANIMATORE DIGITALE E TEAM DIGITALE

- 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

DOCENTE FUNZIONE STRUMENTALE PER LE

NUOVE TECNOLOGIE

- Monitora l'utilizzo delle TIC e segnala al DSGA eventuali problemi che dovessero richiedere acquisti o interventi tecnici;
- Supporta l'attività laboratoriale con

consigli, aiuti e chiarimenti;

- 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

- Pubblicizzare attività formative per i docenti;
- Partecipare ai corsi di formazione per l'acquisizione di idonee competenze teoriche e pratiche;
- 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 rete;

DOCENTI

- Educano 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;

IL PERSONALE ATA

- Acquisisce adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- Prende parte agli incontri formativi promossi dall'ISIS "Valceresio" sulle tematiche della privacy e della digitalizzazione;
- Monitora l'uso di dispositivi tecnologici e attuare politiche scolastiche per quanto riguarda questi dispositivi;
- Segnala 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;

GLI STUDENTI

- Devono leggere, capire e aderire alla e-Policy dell'Istituto;
- Adottano comportamenti rispettosi nella comunicazione in rete

osservando la Netiquette dell'ISIS "Valceresio";

- Utilizzano le TIC su indicazioni del docente;
- Comunicano immediatamente all'insegnante eventuali malfunzionamenti della strumentazione e/o di contatto accidentale con informazioni, immagini e/o applicazioni inappropriate;
- Non devono eseguire tentativi di modifica della configurazione di sistema dei computers;
- 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;
- Chiudono correttamente la propria sessione di lavoro;
- Devono essere consapevoli dei problemi di sicurezza connessi con l'uso di telefoni cellulari, telecamere e dispositivi portatili;
- Sono 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 devono 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.

LE FAMIGLIE

- Partecipare alle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali;
- Relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete;
- comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet.

La corresponsabilità tra genitori e scuola, nel processo di consapevolizzazione e di acquisizione delle competenze per l'uso delle TIC, per quanto riguarda il percorso di crescita delle studentesse e degli studenti è sancita, in particolare, nel 2° comma dell'art. 2048 c.c.:

"I precettori e coloro che insegnano un mestiere o un'arte sono responsabili del danno cagionato dal fatto illecito dei loro allievi e apprendisti nel tempo in cui sono sotto la loro vigilanza"; il 1° comma dell'art. 30 della Costituzione recita inoltre che "è dovere e diritto dei genitori mantenere, istruire ed educare i figli, anche se nati fuori del matrimonio"; il 1° comma dell'art. 2048 c.c. indica che "il padre e la madre o il tutore

sono responsabili del danno cagionato dal fatto illecito dei figli minori non emancipati o delle persone soggette alla tutela, che abitano con essi (...)"; l'art. 147 del c.c. "l'obbligo di mantenere, istruire, educare e assistere moralmente i figli, nel rispetto delle loro capacità, inclinazioni naturali e aspirazioni (...)".

Più precisamente, rispetto ad un profilo prettamente processuale, in materia di bullismo e cyberbullismo, si può parlare di tre tipologie di "culpa" rispetto agli educatori:

o culpa in vigilando: concerne la mancata sorveglianza attiva da parte del docente responsabile verso il minore (cosi come da art. 2048 del c.c.). Tale condizione è superabile se ci si avvale di una prova liberatoria di non aver potuto impedire il fatto (recita il terzo comma dell'art. 2048 c.c.: "le persone indicate nei commi precedenti sono liberate dalla responsabilità soltanto se provano di non aver potuto impedire il fatto").

o culpa in organizzando: si riferisce ai provvedimenti previsti e presi dal Dirigente Scolastico ritenuti come non soddisfacenti e quindi elemento favorevole al verificarsi dell'eventuale incidente.

o culpa in educando: fa capo ai genitori i quali hanno instaurato una relazione educativa con il/la figlio/a, ritenuta come non adeguata, insufficiente o comunque carente tale da metterlo/a nella situazione di poter recare danno a terzi.

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

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

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

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso

improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

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'ISIS "Valceresio": 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 stakeholders, 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.

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

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

L'E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

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

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

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

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.

<u>Dall'a.s. 2024/2025 entra in vigore il codice interno di contrasto al bullismo e al cyberbullismo</u> *ex* art. 4, c. 2-*bis*, legge 29 maggio 2017, n. 71, e s.m.i.

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 E-policy agli alunni:

Attraverso attività, laboratori, incontri, spettacoli che portino a riflettere sui rischi e opportunità del Web.

Condivisione e comunicazione della E-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.

1.5 - Gestione delle infrazioni alla ePolicy

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

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.

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 dell'ISIS "Valceresio" e il regolamento di condotta 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:

- l'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 ridefinizione 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.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

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.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

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:

- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Partecipare al "Safer Internet Day" 2025, la giornata mondiale dedicata all'uso positivo di internet
-

Effettuare interventi all'interno delle classi- referente Ettettuare incontri con lo psicologo d'Istituto Diffondere questionari anonimi e moduli di segnalazione

- Organizzare laboratori didattici per l'approfondimento delle tematiche riconducibili al bullismo e al cyberbullismo in cui gli studenti che hanno affrontato nelle UDA di Educazione Civica.
- Visione lungometraggio Gli Ultimi della Classe", interpretato da ragazzi e
- ispirato alla vera storia di Francesco Scerbo, giovane vittima di bullismo.

Azioni da svolgere nei prossimi 3 anni:

- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti e ai docenti
- Organizzare incontri formativi/informativi con i carabinieri
-
-
-

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.

Le aree di competenza che questo documento si propone di implementare e sviluppare sono quelle individuate dal DigComp e sono, nello specifico:

Area 1: "Alfabetizzazione e dati"

L'area s'inquadra nella dimensione "informazionale" o "cognitiva" delle competenze digitali. Essa è relativa alla capacità di cercare, selezionare, valutare e riprocessare le informazioni in Rete. Nello specifico, per quest'area si dovrebbe puntare a sviluppare negli studenti e nelle studentesse le seguenti competenze:

1. Navigare, ricercare e filtrare dati, informazioni e contenuti digitali;

2. Valutare e gestire dati, informazioni e contenuti digitali;

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

Area 2: "Comunicazione e collaborazione"

Quest'area fa riferimento a quelle competenze volte a riconoscere le giuste ed appropriate modalità per comunicare e relazionarsi online:

1. Saper interagire con gli altri attraverso le tecnologie digitali;

2. Essere consapevoli nella condivisione delle informazioni in Rete;

3. Essere buoni "cittadini digitali";

4. Collaborare adeguatamente con gli altri attraverso le tecnologie digitali;

5. Conoscere le "Netiquette", ovvero le norme di comportamento online;

6. Saper gestire la propria "identità digitale".

Area 3: "Creazione di contenuti digitali"

Quest'area fa riferimento alle capacità di "valutare le modalità più appropriate per modificare, affinare, migliorare e integrare nuovi contenuti e informazioni specifici per crearne di nuovi e originali" (cfr. DigComp 2.1.). Le specifiche competenze digitali che andranno sviluppate in questo caso sono:

1. Creare e modificare contenuti digitali in diversi formati per esprimersi attraverso mezzi digitali;

2. Modificare, affinare, migliorare e integrare informazioni e contenuti all'interno di un corpus di conoscenze esistente per creare conoscenze e contenuti nuovi, originali e rilevanti;

3. Capire come il copyright e le licenze si applicano ai dati, alle informazioni e ai contenuti digitali.

Area 4: "Sicurezza"

Quest'area è parte di una dimensione più generale definita come "benessere digitale" che include la necessità di salvaguardare i propri dati personali e rispettare le regole nel trattare i dati altrui. Nello specifico, bisognerebbe puntare a sviluppare in bambini e ragazzi le seguenti competenze:

1. Imparare a proteggere i dispositivi e i contenuti digitali e comprendere i rischi e le minacce presenti negli ambienti digitali.

2. Conoscere le misure di sicurezza e protezione e tenere in debita considerazione l'affidabilità e la privacy;

2. Proteggere i dati personali e la privacy negli ambienti digitali.

3. Capire come utilizzare e condividere informazioni personali proteggendo se stessi e gli altri dai danni.

4. Comprendere che i servizi digitali hanno un "regolamento sulla privacy" per informare gli utenti sull'utilizzo dei dati personali raccolti;

5. Conoscere (ed esercitare) i propri diritti in termini di privacy e sicurezza.

L'obiettivo che l'ISIS Valceresio si propone è quello di accompagnare gli studenti nell'acquisizione graduale delle competenze digitali, il primo passo di questo processo di apprendimento è connesso alla piena padronanza delle competenze base: la risoluzione di problemi semplici in autonomia, il culmine di questo percorso si propone come intento quello di portare gli studenti e le studentesse a intravedere le possibilità connesse ad un utilizzo creativo delle TIC, ad uno sviluppo delle strategie che permettono la risoluzione di problemi complessi, anche con molti fattori di interazione, possibilità che dischiudono anche opportunità lavorative nuove e innovative.

Gli strumenti che la nostra scuola si propone di utilizzare per raggiungere questi obiettivi sono quelli legati allo svolgimento delle attività didattiche, che, sempre di più utilizzano le TIC per l'organizzazione delle attività didattiche:

- il registro elettronico, con tutte le sue funzioni,
- Google Workspace (Gmail, Google Drive, Google Hangouts, Google Calendar e Google Documenti, ...) come ambiente informatico ad accesso gratuito per la gestione e condivisione di materiale didattico, corsi, prove comuni, consegne
- Video didattici in rete (es. YouTube, OVO, risorse digitali dei manuali in adozione, RAI Scuola, RAI Play)
- Software per la produzione di documenti, fogli di calcolo e presentazioni Software di geometria dinamica (es. Geogebra, Desmos, Tinkercad)
- Software per la didattica collaborativa (es. Padlet, Google Maps, EdModo, Weschool, Etwinning, Pik-to-chart, Storyboard that, Speak-Pic)
- Software per lo sviluppo del pensiero computazionale e il making educativo (es. Cura, pacchetto Autodesk)
- Software per la realizzazione di mappe concettuali (es. CMap) e video tutorial (es. Premiere, Windows media player, Powtoon)
- Software per videoconferenza (Zoom, Skype, ...

Le TIC, sono ad oggi, struttura portante della maggior parte delle attività professionali e del nostro accesso quotidiano alle informazioni e alle comunicazioni, per questo motivo 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.

Integrazione con il curricolo di Educazione Civica

Le RACCOMANDAZIONE DEL CONSIGLIO del 22 maggio 2018 relativa alle competenze chiave per l'apprendimento permanente individuano nell'acquisizione delle competenze digitali un elemento fondamentale per l'esercizio della cittadinanza attiva, pertanto l'Isis Valceresio si propone di integrare, là dove si incontrerà la disponibilità dei cdc, del docente di informatica e dell'animatore digitale, gli argomenti svolti per Educazione Civica con queste tematiche:

Classi prime

Storia, architettura e principi fondativi di Internet

Navigare, ricercare e filtrare dati, informazioni e contenuti digitali

Valutare e gestire dati, informazioni e contenuti digitali

Saper riconoscere e sapersi difendere da contenuti dannosi e pericolosi in rete

Bullismo e Cyberbullismo

Classi Seconde

Saper interagire con gli altri attraverso le tecnologie digitali;

Essere consapevoli nella condivisione delle informazioni in Rete

Collaborare adeguatamente con gli altri attraverso le tecnologie digitali

Conoscere le "Netiquette", ovvero le norme di comportamento online

Saper gestire la propria "identità digitale"

Classi Terze

Creare e modificare contenuti digitali in diversi formati per esprimersi attraverso mezzi digitali

Modificare, affinare, migliorare e integrare informazioni e contenuti all'interno di un corpus di conoscenze esistente per creare conoscenze e contenuti nuovi, originali e rilevanti

Capire come il copyright e le licenze si applicano ai dati, alle informazioni e ai contenuti digitali

Pensiero computazionale

Sexting

Classi quarte

Imparare a proteggere i dispositivi e i contenuti digitali e comprendere i rischi e le minacce presenti negli ambienti digitali

Conoscere le misure di sicurezza e protezione e tenere in debita considerazione l'affidabilità e la privacy

Proteggere i dati personali e la privacy negli ambienti digitali

Conoscere (ed esercitare) i propri diritti in termini di privacy e sicurezza

.

Classi Quinte

Come cambiano organizzazioni, lavoro e professioni? Concetti di moneta e mercato

Come cambiano libertà di espressione, partecipazione e funzionamento della democrazia.

Esercitare la cittadinanza digitale

L'ISIS Valceresio in ottemperanza alle disposizioni della L92/2019 e del DM35/2020

con annesse linee guida, ha integrato il curricolo d'Istituto progettando almeno 33 ore da dedicare all'insegnamento dell'Educazione Civica e ha svilippato già dal 2020 uno dei nuclei fondanti di questa disciplina, l'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 che regolano la vita democratica.

In ottemperanza alla legge 29 maggio 2017, n. 71, e s.m.i. è stato redatto il codice interno

di contrasto al bullismo ed al cyberbullismo e sono stati riorganizzati i gruppi di lavoro: team antibullismo-team per l'emergenza-tavolo permanente di monitoraggio

---

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

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

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

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.

Le problematiche sollevate dall'emergenza COVID impongono alle scuole un sostanziale cambiamento, sia di tipo didattico che di tipo organizzativo.

Per gli aspetti didattici, il punto principale riguarda l'utilizzo della Didattica Digitale Integrata (DDI), che impone ai docenti cambiamenti nelle metodologie e nel processo di insegnamento e apprendimento.

Dal punto di vista organizzativo, assumono particolare importanza le procedure di digitalizzazione della documentazione e dei processi.

Mentre il primo aspetto coinvolge solamente la componente docente, per l'aspetto organizzativo diventa centrale anche il ruolo del personale ATA, soprattutto degli

assistenti amministrativi.

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 dei prossimi tre anni 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.

Si prevede l'attuazione nei prossimi tre anni di un percorso formativo rivolta al personale non docente della scuola, tenuto dal team digitale con la collaborazione degli studenti.

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

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

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.

Al fine di potenziare il livello di competenza nell'uso delle TIC, l'ISIS Valceresio già nel mese di settembre ha proposto ai docenti un corso di formazione: corso B2 Costruire

unità di apprendimento- secondo ciclo Formazione docenti PNFD annualità 2025 ambiti 34 e 35, incentrato sull'integrrazione dei software e delle applicazioni per la costruzione di unità di apprendimento.

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'ISIS Valceresio 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).

Il 20 ottobre del corrente anno scolastico è stato organizzato un incontro con l'ANF Carabinieri di Varese, nel corso dei prossimi tre anni saranno organizzati altri incontri in collaborazione con la Polizia di Stato, la Guardia di Finanza, la Polizia Postale,i Carabinieri sulla sicurezza in rete, reati connessi al cyberbullismo, furto d'identità e frodi online.

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

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

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.

Si prevede l'attivazione di un'apposita sezione sul sito istituzionale della scuola, particolarmente rivolta alle famiglie, con la pubblicazione di materiale informativo e delle procedure per segnalare alla scuola comportamenti non adeguati rispetto alla presente E-policy.

Verrà inoltre attivato, compatibilmente con le risorse a disposizione, un corso di formazione rivolto alle famiglie relativo alle problematiche sull'utilizzo consapevole e sicuro della rete e delle tecnologie digitali, e sulle modalità per la gestione di eventuali problematiche che dovessero nascere con gli adolescenti.

La scuola favorirà inoltre incontri con esperti di associazioni esterne, anche in collaborazione con la rete di scuole, della quale il nostro istituto fa parte, relativa alla prevenzione e al contrasto del bullismo e del cyberbullismo.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2024/2025)

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

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

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali..
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare e promuovere per il corpo docente e per i genitori incontri formativi sull'utilizzo e l'integrazione delle TIC tenuto dagli studenti.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

1. Trattamento dei dati personali e sensibili.

Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc.

In particolare i dati possono essere suddivisi nelle seguenti categorie:

- i dati che permettono l'identificazione diretta di una persona, come i dati anagrafici (ad es. nome e cognome);
- i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad es. il codice fiscale, l'indirizzo IP, il numero di targa);
- i dati rientranti in particolari categorie: si tratta dei dati cosiddetti sensibili, cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale di una persona, i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;
- i dati relativi a condanne penali e reati: si tratta dei dati cosiddetti giudiziari, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad es. i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto o obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

Questi dati subiscono, da parte della scuola, un trattamento tramite le seguenti tipologie di operazioni:

- la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
- Le istituzioni scolastiche pubbliche possono trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali, oppure quelli espressamente previsti dalla normativa di settore. Per tali trattamenti non viene chiesto il consenso al trattamento alle famiglie o agli studenti.

- Alcune categorie di dati personali degli/lle studenti/esse e delle famiglie, come quelli sensibili e giudiziari, devono essere trattate con estrema cautela, nel rispetto di specifiche norme di legge, verificando in primis non solo la pertinenza e completezza dei dati, ma anche la loro indispensabilità rispetto alle "finalità di rilevante interesse pubblico" che si intendono perseguire.
- Periodicamente, almeno una volta durante l'anno scolastico viene effettuata una Valutazione dei rischi sulla privacy: relativamente ad alcune tipologie di trattamento dei dati sensibili
- L'attenzione si focalizza in particolare sui dati sensibili, che la scuola tratta per favorire l'integrazione, come ad esempio dati relativi alle origini razziali.

- Vengono anche esaminate le situazioni che riguardano dati relativi alla salute per adottare misure di sostegno degli alunni o i dati vaccinali con le ATS.
- Per queste particolari categorie di dati viene richiesto espresso consenso alle famiglie o agli studenti, se maggiorenni.
- La scuola annualmente fornisce una lettera di incarico per il trattamento dei dati al personale ATA, ai collaboratori scolastici e ai docenti.

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'Isis "Valceresio" si avvale della consulenza di esperti nel settore della tutela della privacy.

2. Sito web istituzionale di riferimento e infrastrutture tecnologiche della scuola

- Viene programmato il passaggio all'utilizzo del protocollo HTTPS (l'Hypertext Transfer Protocol Secure) per garantire maggior sicurezza nelle transazioni sul sito della scuola.
- Viene utilizzato un sistema di cifratura quando il trattamento di dati lo richiede (ovvero oscurare il dato per renderlo incomprensibile a coloro che non hanno i codici per accedervi, mediante la "crittografia" e, quindi, l'uso di un algoritmo di cifratura).
- In particolare tutte le transizioni su GSUITE sono criptate.
- L'accesso alla rete Wifi dell'istituto prevede due fattori di protezione: l'utilizzo di una password e l'autorizzazione al singolo dispositivo.
- E' prevista in tutti i punti di accesso alla rete Internet, la presenza di firewall hardware con un sistema di filtraggio dei contenuti e meccanismi di prevenzione da intrusioni esterne.
- L'accesso a tutti i dispositivi hardware che memorizzano dati personali è protetto da UserName e Password, che gli utilizzatori provvedono a cambiare periodicamente.
- E' previsto un sistema di backup incrementale periodico di tutti i dati

contenuti nel server degli uffici, su dispositivo di memorizzazione esterno, che viene conservato in apposito armadio blindato, in un locale separato.

- I docenti, per l'acceso al registro elettronico sono dotati di UserName e Password personale e hanno acceso soltanto ai dati indispensabili e relativi alla propria attività nelle proprie classi.
- Soltanto il personale di segreteria ha accesso ai dati memorizzati sul server d'Istituto, relativi a studenti, famiglie, personale. Ogni assistente amministrativo ha accesso soltanto ai dati strettamente correlati con la funzione svolta.

3. 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 e l'accesso ad internet è consentito a scopi didattici al personale docente attraverso l'assegnazione di una password personale.

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.

3.2 - Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*

3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

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

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

Attualmente il nostro Istituto non è raggiunto da fibra ottica, ma consente l'accesso a Internet attraverso una rete LAN e Wi-Fi abbastanza adeguata ed in grado di supportare il traffico dati generato da un numero elevato di utenti. L'accesso ad Internet, protetto da software antivirus, è consentito:

- al personale docente e non docente per uso didattico e/o di formazione;
- agli alunni, dagli appositi laboratori, per lo svolgimento delle attività didattiche proposte, guidate dal docente e sotto la sua responsabilità.

Per garantire maggiore sicurezza nell'accesso ai dati sensibili, le reti didattica e segreteria sono mantenute separate, gestite in modo autonomo e con regole differenti.

Si rammenta che, a norma delle leggi vigenti, l'utente è responsabile direttamente, civilmente e penalmente, dell'uso effettuato del servizio Internet.

Nelle aule l'accesso avviene tramite rete LAN, è protetto da password e le credenziali non sono fornite agli alunni, ma comunicate ai Docenti; le attività sulle postazioni fisse dei laboratori e nelle LIM sono vigilate e mediate dai Docenti.

Per quanto riguarda l'accesso ad Internet all'interno dei laboratori dell'Istituto si rimanda agli specifici regolamenti di accesso e di utilizzo vigenti approvati, consultabili sul sito della scuola.

Gli assistenti tecnici periodicamente provvedono alla manutenzione ed all'aggiornamento del sistema e degli antivirus installati, richiedendo, ove necessario, l'intervento di tecnici esterni.

La posta elettronica istituzionale, assegnata ad ogni docente e al personale ATA, è protetta da antispam ed è fornita Aruba.

Al fine di garantire il diritto di accesso a Internet in condizioni di sicurezza, l'istituto ha considerato la prevenzione dei rischi in rete, in termini di uso consapevole delle tecnologie digitali e mediante i protocolli di sicurezza che rendono accessibile l'ambiente digitale, dall'antivirus ai firewall, all'aggiornamento periodico dei sistemi operativi e browser, dei software gestiti dai server, per garantire che il sistema sia aggiornato e protetto dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo.

La scuola ha dunque adottato le necessarie precauzioni per evitare l'accesso on line da parte di studenti e studentesse a materiali non adatti a loro all'interno della scuola, attraverso l'adozione di sistemi di filtraggio, hardware (filtraggio dei contenuti).

Si invita quindi l'intera comunità scolastica a rispettare le seguenti linee guida di buona condotta/buone pratiche:

- rispetto della legislazione vigente;
- tutela della propria privacy, di quella degli altri utenti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui si ha accesso;
- rispetto di una netiquette cioè di regole condivise che disciplinano il rapportarsi fra utenti della rete, siti, forum, mail e qualsiasi altro tipo di comunicazione a distanza;
- controllo della validità e dell'origine delle informazioni a cui si accede o che si ricevono; rispetto dei diritti di autore e dei diritti di proprietà intellettuale;
- divieto di installare e/o scaricare sui device software non autorizzati o senza licenza; accesso consentito al personale scolastico ad esclusivo uso didattico o di formazione; accesso consentito agli alunni sotto la responsabilità di un docente.

Nel caso in cui un docente preveda l'utilizzo di Internet all'interno dell'attività didattica è opportuno che:

- dia chiare indicazioni agli studenti sul corretto utilizzo della rete;
- si assuma la responsabilità di segnalare prontamente all'Ufficio Tecnico e/o all'animatore digitale eventuali malfunzionamenti/danneggiamenti o l'utilizzo improprio della rete;
- non salvi sui computer dell'Istituto files contenenti dati personali e/o sensibili;
- filtri i contenuti in base all'età e ruolo dell'utente;
- usi pw personali di accesso forti e non vulnerabili (almeno 8 caratteri con numeri, caratteri maiuscoli e minuscoli e caratteri speciali);
- non memorizzi pw sui dispositivi scolastici; non condivida le pw con nessuno.

Durante l'emergenza epidemiologica l'Istituto ha fornito in comodato d'uso dei tablet a studenti in situazione di svantaggio socio-economico e/o in condizioni di difficoltà di ordine tecnologico (assenza di device, problemi di cogestione di dispositivi da parte di più membri della famiglia).

3.3 - Strumenti di comunicazione online

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

Strumenti di comunicazione esterna dell'"Isis Valceresio":

- il sito web, dove sono reperibili contenuti specificamente rivolti a studenti, docenti, genitori e personale ATA (informazioni e modulistica), link a siti e servizi attinenti la scuola, informazioni e documenti circa il funzionamento della scuola e l'attività didattica.
- il registro elettronico, che consente di gestire in tempo reale la comunicazione con le famiglie, le quali attraverso di esso possono visualizzare molte informazioni utili, interagendo con la scuola sui seguenti aspetti: andamento scolastico (rilevazione presenze e assenze di studenti e docenti, argomenti svolti e compiti assegnati, eventuali note disciplinari), risultati scolastici (valutazioni delle prove, giudizi, documenti di valutazione intermedi e finali), prenotazioni colloqui individuali, eventi e calendarizzazione delle lezioni

e delle verifiche, comunicazione varie (comunicazioni di classe, comunicazioni personali e del Dirigente scolastico). L'accesso e la compilazione del RE da parte dei docenti obbedisce a regole e tempistiche particolari, al fine di mettere in atto una comunicazione tempestiva e, dunque, efficace.

Sono attivi profili social, ma non newsletter, né blog.

Strumenti di comunicazione interna ed esterna del nostro Istituto:

- Google Suite for Education (GS4E): questo applicativo, usato prima dell'emergenza sanitaria manifestatasi a fine febbraio 2020, soprattutto per una comunicazione interna attraverso un account fornito a tutto il personale docente, amministrativo, tecnico e dirigenziale dell'Istituto, e attraverso l'uso di Drive per condividere materiali e modulistica, è diventato strumento anche per la comunicazione esterna rivolta agli studenti e alle famiglie (uso della piattaforma Classroom e dell'applicativo Meet per attività di didattica digitale integrata, riunioni degli organi collegiali, riunioni di gruppi di lavoro, formazione del personale, colloqui scuola-famiglia).

3.4 - Strumentazione personale

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

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

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

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 nell'arco dell'anno scolastico 2024/2025).

Scegliere almeno 1 di queste azioni:

- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

Scegliere almeno 1 di queste azioni:

- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

I rischi on line rappresentano tutte le situazioni problematiche derivanti da un uso non consapevole e non responsabile delle Tecnologie Digitali da parte degli studenti, in particolare di quelli minorenni: adescamento online, cyberbullismo, sexting, violazione della privacy, pornografia, pedopornografia, gioco d'azzardo o gambling, internet addiction, videogiochi online, esposizione a contenuti dannosi o inadeguati (ad es.

contenuti razzisti, che inneggiano al suicidio, che promuovono comportamenti alimentari scorretti, ecc.).

Cornelius Williams, Direttore associato dell'UNICEF per i programmi di protezione dell'infanzia, pone la sua attenzione proprio sul fatto che «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»,il rapporto, infatti, 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.

Vanno dunque promosse nei più giovani le necessarie conoscenze, competenze e capacità, al fine di una protezione adeguata, ma anche di un utilizzo consapevole che sappia sfruttare le potenzialità delle Tecnologie Digitali e gestirne le implicazioni.

La sensibilizzazione costituisce il primo passo verso un cambiamento positivo, affinché possa avere una sua efficacia è importante impegnarsi:

- in un **primo momento** su interventi che permettono di considerare con chiarezza lo stato della situazione attuale al fine di acquisire la **consapevolezza dello status quo**;
- in un **secondo momento** sull'organizzazione di incontri o attività volti a innescare la **motivazione al cambiamento**;
- in un **terzo momento** sulla scelta delle azioni da porre in essere al fine di **produrre il cambiamento**.

Le azioni di Sensibilizzazione che il nostro Istituto intende intraprendere sono:

- attivare percorsi/incontri educativi sui rischi della rete sia per gli studenti che per i genitori avvalendosi del personale della scuola con competenze specifiche, ma anche di personale esterno alla scuola (Polizia postale, forze dell'ordine, servizi sociali, psicologi, educatori, ecc.) per accrescere negli studenti e nelle studentesse la consapevolezza di particolari problemi relativi ad un uso improprio dell'on line, ma anche per rendere alunni e alunne consci dell'importanza di denunciare comportamenti sbagliati cui assistono o partecipano;
- favorire la diffusione di informazioni e servizi disponibili all'utilità collettiva (ad esempio, promuovere la conoscenza dell'E-policy nella comunità scolastica, promuovere la conoscenza di siti utili come Generazioni Connesse, le attività dell'Help line di Telefono Azzurro, del Co.Re.Com, l'applicazione App to Young).

Le azioni di Prevenzione che il nostro Istituto intende intraprendere per prevenire la delicata problematica dei rischi online sono:

- attivare percorsi di educazione civica digitale al fine di formare e consolidare le competenze educative di base necessarie a poter gestire le situazioni online e per un uso consapevole della rete (vedasi, a questo proposito, quanto esplicitato nel capitolo 2);
- progettare attività, azioni ed interventi 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 degli studenti.
- presentare e rendere disponibile sul sito dell'istituto, sulle pagoine facebook e instagram l'accesso ai servizi dell'App to Young

Qui di seguito alcuni suggerimenti utili in un'ottica di prevenzione dei rischi on line:

- osservare in modo critico e attento i siti visitati;
- non dichiarare la propria identità;
- non condividere notizie riservate;
- non scaricare applicazioni o video o musica;
- non accettare l'installazione di script;
- non cliccare sui link o sui banner pubblicitari;
- quando si naviga, tenere aggiornato il browser e dopo avere visitato qualche sito sospetto eliminare i cookie (fare pulizia del browser);
- leggere sempre l'indirizzo del mittente delle e-mail, anche quando il logo che compare sullo schermo risulta familiare.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

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

La stessa legge e le relative **Linee di orientamento per la prevenzione e il contrasto del cyberbullismo** indicano al mondo scolastico ruoli, responsabilità e

azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
  - Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
  - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

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

1. **cyberbullismo diretto**: il bullo utilizza strumenti di messaggistica istantanea 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, ma 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.

Come riconoscere casi di cyberbullismo?

Di seguito, alcuni segnali generali che può manifestare la potenziale vittima di cyberbullismo:

- appare nervosa quando riceve un messaggio o una notifica;

- sembra a disagio nell'andare a scuola o finge di essere malata (ha spesso mal di stomaco o mal di testa);
- cambia comportamento ed atteggiamento in modo repentino;
- mostra ritrosia nel dare informazioni su ciò che fa on line;
- soprattutto dopo essere stata on line, mostra rabbia o si sente depressa;
- inizia ad utilizzare sempre meno pc e telefono (arrivando ad evitarli);
- perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;
- il suo rendimento scolastico peggiora.

Un'altra indicazione operativa concerne una valutazione circa l'eventuale stato di disagio vissuto dalla/e persona/e minorenne/i coinvolta/e, per cui potrebbe essere necessario rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza (ad esempio: spazio adolescenti, se presente, del Consultorio Familiare, servizi di Neuropsichiatria Infantile, centri specializzati sulla valutazione o l'intervento sul bullismo o in generale sul disagio giovanile, e sui comportamenti a rischio in adolescenza, ecc.).

La Legge 71/2017 introduce un provvedimento di carattere amministrativo per gli autori di atti di cyberbullismo.

Più precisamente si tratta della procedura di ammonimento prevista in materia di stalking (art. 612- bis c.p.), in caso di condotte di ingiuria (art. 594 c.p.), diffamazione (art. 595 c.p.), minaccia (art. 612 c.p.) e trattamento illecito di dati personali (art. 167 del codice della privacy) commessi mediante Internet da minori ultraquattordicenni nei confronti di altro minorenne, se non c'è stata querela o non è stata presentata denuncia. Questa procedura è stata estesa al cyberbullismo e può essere impartita da parte del questore che convoca il minore, insieme ad almeno un genitore o a chi esercita la responsabilità genitoriale. Gli effetti dell'ammonimento cessano al compimento della maggiore età.

Chi compie atti di bullismo e cyberbullismo può anche essere responsabile di reati penali e danni civili. Secondo il codice penale italiano i comportamenti penalmente rilevanti in questi casi sono:

- percosse (art. 581),
- lesione personale (art. 582), ingiuria (art. 594),
- diffamazione (art. 595), violenza privata (art. 610), minaccia (art. 612),
- danneggiamento (art. 635).

Questi atti devono essere non occasionali, avvenuti in presenza di un pubblico, tra coetanei, in modo cronico ed intenzionale.

La legge punisce gli atti di violenza e di cyberbullismo: nei casi più gravi basta la denuncia ad un organo di polizia o all'autorità giudiziaria per attivare un procedimento penale (per es. lesioni gravi, minaccia grave, molestie); negli altri casi, la denuncia

deve contenere la richiesta che si proceda penalmente contro l'autore di reato (querela).

Per poter avviare un procedimento penale nei confronti di un minore è necessario:

- che abbia almeno compiuto 14 anni;
- che, anche se maggiore di 14 anni, fosse cosciente e volente al momento del comportamento, cioè in grado di intendere e volere (tale non sarebbe, per esempio, un ragazzo con degli handicap psichici).

L'atto di bullismo può violare sia la legge penale, sia quella civile, quindi può dar vita a due processi, l'uno penale e l'altro civile.

Parallelamente, nel caso in cui si ipotizzi che ci si possa trovare di fronte ad una fattispecie di reato (come, ad esempio, il furto di identità o la persistenza di una condotta persecutoria che mette seriamente a rischio il benessere psicofisico del bambino/a o adolescente coinvolto/a in qualità di vittima) si potrà far riferimento agli uffici preposti delle Forze di Polizia per inoltrare la segnalazione o denuncia/querela e permettere alle autorità competenti l'approfondimento della situazione da un punto di vista investigativo. È in tal senso possibile far riferimento a queste tipologie di uffici: Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza;Polizia di Stato – Commissariato on line (attraverso il portale http:// www.commissariatodips.it).

Inoltre, per un consiglio e un supporto è possibile rivolgersi alla Helpline di Telefono Azzurro per Generazioni Connesse: operatori esperti e preparati sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che dei/lle bambini/e, degli adolescenti, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti l'utilizzo dei media digitali.

Le responsabilità per atti di bullismo e cyberbullismo compiute dal minorenne possono ricadere anche su:

- i genitori, perché devono educare adeguatamente e vigilare, in maniera adeguata all'età del figlio, cercando di correggerne comportamenti devianti. Questa responsabilità generale persiste anche per gli atti compiuti nei tempi di affidamento alla scuola (culpa in educando).
- gli insegnanti e la scuola, perché nei periodi in cui il minore viene affidato all'Istituzione scolastica il docente è responsabile della vigilanza sulle sue azioni e ha il dovere di impedire comportamenti dannosi verso gli altri/e ragazzi/e, insegnanti e personale scolastico o verso le strutture della scuola stessa. A pagare in primis sarà la scuola, che poi potrà rivalersi sul singolo insegnante. La responsabilità si estende anche a viaggi, gite scolastiche,

manifestazioni sportive organizzate dalla scuola, ecc. (culpa in vigilando).

- la scuola, quando non mette in atto le azioni previste per la prevenzione del fenomeno o per affrontarlo al meglio, così come previsto anche dalla normativa vigente (culpa in organizzando).

L'Isis "Valceresio" ritiene che solo interventi sinergici e condivisi sia sul piano verticale che orizzontale possano prevenire o affrontare gli atti del bullismo online, nella consapevolezza che le azioni efficaci debbano ricorrere agli strumenti educativi, rieducativi e di mediazione del conflitto, supportati anche da azioni di comunicazione e informazione di natura giuridica sulle responsabilità da conoscere intorno alla possibilità di commettere reati o danni civili.

Per questo, in merito alle azioni di prevenzione e contrasto da sviluppare a scuola, si farà riferimento alle indicazioni contenute nella Legge 71/2017, Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo, approvata dal Parlamento il 18 maggio 2017 e alle Linee di orientamento per la prevenzione e il contrasto del cyberbullismo, documenti che indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo.

Nell'Istituto opera un Referente per il contrasto al bullismo e cyberbullismo che monitora la situazione e cui i docenti fanno riferimento per realizzare, all'interno dell'azione curricolare e nel caso si verifichino episodi riconducibili a casi di cyberbullismo, percorsi di riflessione e dialogo con l'intero gruppo classe.

Inoltre, ritenendo che l'informazione e la sensibilizzazione siano le misure più efficaci per prevenire il più possibile il cyberbullismo, l'Istituto curerà iniziative di formazione e sensibilizzazione rivolte a studenti, docenti e genitori, con l'eventuale coinvolgimento dei servizi socio-educativi del territorio.

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

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante

affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

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

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

E' difficile individuare e definire in maniera netta un "discorso di incitamento all'odio": i criteri per riconoscerlo non sono definibili a priori e, di conseguenza, le misure per arginarlo non sono immediate.

Un'indicazione pragmatica per individuarlo: chiedersi quali conseguenze comporterebbe per tutte le parti coinvolte non prendere misure per contenere o contrastare le espressioni in questioni. Non agire, implica che siano accettabili, o tollerabili.

L'azione di contrasto a un contenuto potenzialmente dannoso pubblicato sul Web è frenata dalla possibile interferenza con la "libertà di espressione", principio dai margini talmente sottili da essere, a sua volta, molto difficile da definire.

L'isis "Valcersio", considerando le possibili conseguenze di questo fenomeno su personalità in formazione come quelle delle studentesse e degli studenti che frequenytano la scuola, intende mettere in campo un piano d'azione immediato ed efficace, accogliendo la definizione proposta dal Consiglio d'Europa:

The term "hate speech" shall be understood as covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin.

Recommendation No. R (97) 20 of the Committee of Ministers to Member States on "Hate Speech"

- La definizione del discorso di incitamento all'odio proposta dal Consiglio d'Europa copre "tutte le forme di espressione", quindi, in altri termini, non solo sotto forma di parole, ma anche di immagini, video, o di qualsiasi altra attività online. L'odio diffuso in rete rientra quindi nella fattispecie del discorso di incitamento all'odio

- Nella definizione del Consiglio d'Europa si utilizzano i verbi: diffondere, incitare o promuovere: verbi che rimandano agli obiettivi che l'autore di un

discorso di incitamento all'odio vuole produrre intenzionalmente. Non si tratta quindi di un semplice insulto, ma del tentativo di produrre un effetto concreto sulla vittima di Hate Speech

- Inoltre il Discorso di incitamento all'odio, per essere tale, deve avere come obiettivo uno specifico gruppo di persone. In questa definizione si parla in particolare di minoranze etniche e religiose. Si possono inoltre aggiungere altre categorie di gruppi a rischio di discriminazione: donne, anziani, giovani, diversamente abili e persone LGBTI (Special Eurobarometer 437. Discrimination in the EU in 2015).

  In conclusione, un Hate Speech è tale se produce degli effetti concreti sulle vittime e se si rivolge a gruppi di persone a rischio di discriminazione

Come riconoscerlo?

Il discorso dell'odio si manifesta con un ampio spettro di azioni: sebbene tutte le espressioni che istigano all'odio meritino di essere classificate come malvagie, ne esistono alcune che possono essere peggiori di altre. Certe espressioni di odio sono più estreme, utilizzano termini più insultanti e possono perfino istigare altri ad agire, altre contengono insulti più moderati o generalizzazioni eccessive.

Come prevenirlo?

Il nostro Istituto, al fine di prevenire o affrontare tale fenomeno, fonda la sua azione su un curricolo verticale che si declina in percorsi/progetti didattici-educativi quali "cittadinanza e costituzione" e "cultura e legalità" intorno ai temi dell'intercultura, dei diritti e doveri, dello sviluppo storico del pregiudizio culturale, del riconoscimento delle fake news, nell'analisi dei codici comunicativi dei media, del rispetto ambientale e sociale, dell'inclusione e del dialogo attivo e partecipe, della condivisione delle buone regole di comportamento basate sul rispetto della persona.

Si tratta di un fenomeno che si radica in dinamiche profonde e si manifesta anche attraverso riferimenti sottili, alle volte invisibili per l'occhio del docente, l'Isis Valceresio, si propone, comunque di mettere in atto un piano di intervento per contrastare questo fenomeno:

- analizzare i siti che manifestano questo tipo di odio e sensibilizzare gli alunni mediante la realizzazione di attività (per esempio slogan pubblicitari) che indicano questi siti mettendoli al bando;
- sensibilizzare gli alunni mediante campagne di educazione e formazione con esposizione di risultati indicativi su possibili azioni e soluzioni;
- valorizzare la dimensione relazionale dei più giovani, attraverso un loro coinvolgimento attivo anche in problematiche che riguardano la scuola, sensibilizzandoli alla capacità di analisi e discernimento;
- fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su

cui spesso si fondano forme di hate speech, come ad esempio attività di analisi e produzione attraverso i media;

- promuovere negli alunni la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- sviluppare le competenze digitali degli alunni e l'educazione ad un uso etico e consapevole delle tecnologie;
- sostenere le vittime di abusi e discriminazione di questo tipo;
- ridurre il linguaggio comprendente termini che facciano riferimento alla discriminazione e all'odio;
- educare ad un uso corretto delle piattaforme sociali;
- esortare chi subisce tali vessazioni a parlare con un docente, un adulto di fiducia o con il referente della scuola;
- denunciare alle forze dell'ordine i siti o le persone che proclamano incitazioni all'odio e alla discriminazione;
- esortare i ragazzi a cercare di dissuadere amici che usano l'hate speech o lo giustificano, richiedendo contestualmente l'aiuto di un adulto di riferimento.

4.4 - Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

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

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.

Tra le varie forme di benessere a scuola, naturalmente viene incluso anche quello digitale.

Per poterne favorire il raggiungimento, è opportuno rendere consapevoli tutti gli attori

della vita scolastica dei sintomi e delle forme di prevenzione della dipendenza da Internet. La Società Italiana Intervento Patologie Compulsive, definisce la dipendenza da Internet come progressivo e totale assorbimento del soggetto alla Rete. Spesso la permanenza disfunzionale in rete si lega anche a forme di Dipendenza dal gioco online (Net gaming addiction o Internet Gaming Addiction), intesa come un utilizzo continuativo e sistematico della Rete al fine di giocare impegnando la maggior parte delle giornate, con la conseguente sottrazione del tempo alle altre attività quotidiane del minore.

Come riconoscere una dipendenza?

Si può parlare di dipendenza quando la maggior parte del tempo e delle energie vengono spesi nell'utilizzo della rete, creando in tal modo menomazioni forti e disfunzionali nelle principali e fondamentali aree esistenziali, come quella personale, relazionale, scolastica, familiare, affettiva.

La S.I.I.Pa.C., la Società Italiana Intervento Patologie Compulsive, definisce la dipendenza da Internet come progressivo e totale assorbimento del soggetto alla rete; di seguito alcune caratteristiche specifiche:

- Dominanza: l'attività domina i pensieri ed il comportamento del soggetto, assumendo un valore primario tra tutti gli interessi
- Alterazioni del tono dell'umore: l'inizio dell'attività provoca cambiamenti nel tono dell'umore; il soggetto prova un aumento d'eccitazione o maggiore rilassatezza come diretta conseguenza dell'incontro con l'oggetto della dipendenza
- Conflitto: conflitti inter-personali tra il soggetto e coloro che gli sono vicini, conflitti intrapersonali
- Ricaduta: tendenza a ricominciare l'attività dopo averla interrotta.

I segnali patologici di questo che viene descritto come "un vero e proprio abuso della tecnologia", anche denominato "Internet Addiction Disorder" (I.A.D.), sono specifici così come accade per le altre dipendenze più note e possono essere così riassunti:

- la **tolleranza**, ossia quando vi è un crescente bisogno di aumentare il tempo su Internet
- l'**astinenza** quando, cioè, vi è l'interruzione o la riduzione dell'uso della rete che comporta ansia, agitazione psicomotoria, fantasie, pensieri ossessivi (malessere psichico e/o fisico che si manifesta quando s'interrompe o si riduce il comportamento).

Tutto questo ha ripercussioni sulla sfera delle relazioni interpersonali che diventano via via più povere e alle quali si preferisce il mondo virtuale, con alterazioni dell'umore e della percezione del tempo.

Spesso il trascorrere del tempo on line, in termini disfunzionali, è scandito dal gioco

virtuale che può anche assumere forme di Dipendenza dal gioco online (Net gaming addiction o Internet Gaming Addiction) inserito all'interno del Manuale Diagnostico Statistico dei Disturbi Mentali (DSM5).

Da specificare che la dipendenza si realizza quando c'è un **abuso**, ossia un utilizzo continuativo e sistematico della rete al fine di giocare impegnando la maggior parte delle giornate, con la conseguente sottrazione del tempo alle altre attività quotidiane del minore.

Per il gioco d'azzardo il fenomeno della dipendenza è più pericoloso in quanto prima dell'avvento di Internet questo "vizio" si acquisiva solo con la frequentazione di luoghi predisposti a tali giochi; oggi invece avere una possibilità dei connessione alla rete sempre e dovunque a disposizione, favorisce il fenomeno e l'innesco del vizio e di conseguenza la dipendenza. Questo in termini scientifici si chiama IGD (Internet Gaming Disorder).

Come contrastare queste forme di dipendenza?

Queste dipendenze possono essere contrastate se il soggetto ammette la dipendenza, così si potrà procedere alla definizione del livello di dipendenza individuando i pensieri disadattivi: generalizzazione, astrazione selettiva, esaltazione. Segnali che possono portare a individuare queste dipendenze sono espressioni (ripetute/iterate) come: "off line non sono nessuno ma on line sì"; "Nessuno mi ama off line"; "Il mondo del gioco on line è l'unico posto dove sono rispettato"; "Ho una certa reputazione online"…

Queste problematiche complesse devono essere trattate per via terapeutica da personale specializzato o da strutture appositamente fornite di tale personale. In via preventiva nell'ambito della prevenzione primaria, con interventi psico-pedagogici sistematici e ben strutturati di promozione alla salute, che potenziano le life skills secondo le indicazioni dell'OMS.

Qual è il piano d'azione dell'isis "Valceresio"

- riflettere con i ragazzi e le ragazze rispetto all'uso della tecnologia in termini di qualità e tempo (ad esempio attraverso questionari da sottoporre loro per investigare sul disturbo psicopatologico legato all'abuso di Internet), affinché gli studenti e le studentesse siano consapevoli delle proprie abitudini online e dei rischi che comporta l'iperconnessione.

La linea d'azione del nostro istituto non intende demonizzare il gioco online o l'uso delle TIC, nella consapevolezza che questi strumenti possono costituire aperture di senso e di nuove dimensioni di possibilità per gli studenti e le studentesse nel momento in cui l'approccio sia consapevole, positivo e controllato, perciò si propone di aprire un dialogo con le classe,

- per provare a comprendere il mondo degli studenti e delle studentesse,
- per aiutarli ad acquisire consapevolezza della sovrapposizione del piano

virtuale e del piano di realtà,

Al fine di

- individuare insieme a loro chiare e semplici regole condivise di utilizzo,
- considerare ed acquisire delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d'aula (Es. adoperando la LIM).

Mantenere un dialogo aperto con le classi e con le famiglie consente anche di cogliere segnali che possono far sospettare un'iperconnessione o l'attività del gioco d'azzardo on line. Particolarmente importante risulta dunque il rapporto scuola- famiglia, percorso educativo effettivamente sinergico.

L'isis Valceresio si propone, inoltre di selezionare momenti di formazione con esperti esterni che siano in grado di indicare strategie per un uso più consapevole delle tecnologie per favorire il "benessere digitale", cioè la capacità di creare e mantenere una relazione sana con la tecnologia.

Le attività di formazione possono essere:

- 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;

4.5 - Sexting

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti mediali sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i

protagonisti delle immagini, delle foto e dei video.

La parola sexting (abbreviazione di sex – sesso e texting – inviare messaggi) è stata certificata nel 2009 ed indica l'invio e/o la ricezione di contenuti (video o immagini) sessualmente espliciti che ritraggono se stessi o gli altri.

Spesso sono realizzati e vengono diffusi attraverso il cellulare o attraverso siti, e-mail, chat; tali immagini o video, anche se inviate ad una persona o a una cerchia ristretta, si diffondono in modo incontrollabile e possono creare seri problemi, sia personali che legali, alla persona ritratta.

L'invio di immagini o video che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico; i contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di "**revenge porn**" letteralmente "vendetta porno" fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte.

Questa pratica, che inizia come un gioco e poi si trasforma per alcuni in un mezzo di aggressione verso le loro vittime, nel tempo può finire con il danneggiare, sia in termini psicologici che sociali, sia il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che hanno contribuito a diffonderla. Le ripercussioni negative sulla vittima possono essere in termini di autostima, di credibilità, di reputazione sociale off e on line, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro, depressione ed abuso di sostanze o di alcool.

Qual è il piano d'azione dell'Isis Valceresio?

La nostra scuola per prevenire ed affrontare la delicata problematica del sexting si propone di:

- integrare i corsi, anche nell'ambito dell'Educazione Civica, con contenuti informativi sui temi legati all'affettività, alla sessualità e alle differenze di genere, secondo le età degli alunni e delle alunne, anche con il supporto di esperti esterni;
- comunicare con chiarezza agli alunni e le alunne il protocollo da seguire e le persone di riferimento in caso di revenge porn subito o di cui si è venuti a conoscenza;
- attuare campagne informative verso gli alunni e le alunne sui rischi anche penali che questa pratica può comportare essendo una violazione della sicurezza e della privacy delle persone;
- proporre ai docenti, e, quindi, agli studenti, percorsi di riflessione e confronto su questa tematica;
- rendere disponibilile sul sito ufficiale della scuola e sulle pagine social della

scuola contenuti informativi per studentti, genitori e docenti;

- consigliare ai genitori di parlare con i propri figli sull'uso della tecnologia e sui pericoli che possono crearsi in Internet;
- fornire loro informazione circa le possibilità di attivare forme di controllo parentale della navigazione e sensibilizzare sulla necessità di monitorare la presenza sui social dei figli;
- formare e supportare i docenti all'uso della tecnologia che usano gli studenti.

4.6 - Adescamento online

Il ***grooming*** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di ***teen dating*** (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

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

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

"La rete non è un luogo sicuro – ha detto l'ex capo della polizia Franco Gabrielli - Internet non è una dimensione immateriale, i comportamenti che teniamo hanno ricadute sulle vite delle persone", il grooming, insieme al revenge porn e alle conseguenze dell'hate speech ne sono testimonianza diretta.

Il grooming, nello specifico, è un percorso lungo che si articola in più momenti:

1. **Contatto**: l'adulto cerca la conversazione con il minore contattandolo attraverso i social e proponendo una conversazione su temi generali (sport,

giochi, scuola, etc.);

2. **Fiducia**: l'adulto cerca di instaurare una relazione privata introducendo argomenti più familiari facendosi raccontare delle storie e poi si propone come un amico/confidente, si informa sul livello di libertà che l'adolescente ha nell'uso di Internet, cerca di fare dei regali,di scambiare immagini (anche di tipo sessuale);
3. **Esclusività**: l'adulto cerca di creare un ambiente confidenziale e di isolare così il minore dall'ambiente esterno (amici, scuola, famiglia), cerca di avere un contatto o incontro off line. Per ottenere il silenzio del minore gli fa credere che quella situazione sia normale o che è stata per la sua volontà; può minacciare il minore della pubblicazione delle immagini/video.

Il bambino/a o l'adolescente coinvolto in quel momento particolare della sua vita in cui deve fare i conti con un corpo che cresce e nel quale non si riconosce più appieno, con delle relazioni tra pari, alle volte, difficili e critice, cade facilmente in una trappola così ben strutturata: un rapporto esclusivo, accudiente e focalizzato sulla sua vita.

Come può l'Isis "Valceresio" far fronte a questo fenomeno?

Da un lato proponendo una riflessione sulla relazione interpersonale genitore-figlio, docente-insegnante, nella consapevolezza che l'adulto può, attraverso il dialogo educativo, rendere il minore attento:

- a non fidarsi di chi vuole sapere troppe cose, non dare informazioni private (famiglia, amici), non inviare foto, non parlare con chi non si conosce, ricordare che Internet è immateriale quindi dall'altra parte ci può essere chiunque;
- al fatto che on line sia facile mentire, alcune persone fingono di essere quelle che in realtà non sono (coetanei) o non dire la verità;
- a non esporsi accettando incontri con chi non si conosce, a non accettare foto perchè possono essere contraffatte;
- al proprio sentire: se la situazione è di disagio interrompere il collegamento e bloccare il contatto e parlare con un adulto;

Da un altro lato attraverso la formazione e la diffusione a studenti e famiglie dei vantaggi dell'uso della tecnologia, che può aiutare

- il **controllo**:
  - l'uso dello smartphone deve prevedere delle regole,
  - strumenti e applicazioni permettono di installare l'icona sul cellulare del figlio e l'app gemella sul telefono del genitore che riceve notifiche, posizione, mail inviate, aggiunte di numeri in rubrica;
- l'**informazione:**
  - online ci sono tante offerte di aiuto, istruzioni per la navigazione famigliare, assistenza psicologica, c'è l'aiuto della polizia postale, ci

sono tutorial su YouTube. La Fondazione Carolina (intitolata a Carolina Picchio, vittima del cyberbullismo nel 2013) ha realizzato una guida per minori online che si può scaricare gratis e raccoglie molte informazioni sui vari social, età di accesso e regole (su TikTok, ad esempio, un genitore può collegarsi all'account del figlio adolescente, anche per stabilire un tempo massimo di connessione)

Da un altro lato ancora attraverso dei **corsi e dei percorsi di formazione**, anche gestiti da esperti esterni, volti a:

- accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità, al fine di renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, ed imparare, innanzitutto, a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri;
- sensibilizzare studenti e studentesse, attraverso momenti formativi dedicati, sull'importanza della privacy, su tutti gli aspetti e le azioni che configurano il reato di adescamento e sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, non corrette con i minori;
- mettere a disposizione degli alunni un canale di comunicazione e/o sportello/BOX per eventuali preoccupazioni/segnalazioni/dubbi in merito.
- fornire loro la sicurezza che li renda consapevioli e capaci di agire anche quando pensano di aver fatto un errore.
- proporre agli adulti coinvolti, genitori e docenti, una prospettiva scevra dal giudizio, che li renda punti di riferimento di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato.

Si fa inoltre presente che, all'interno dell'Istituto, oltre al Dirigente Scolastico e ai docenti, operano un Referente per azioni di contrasto al bullismo e cyberbullismo e uno psicologo scolastico (Sportello di Ascolto), con il compito di accogliere/supportare gli studenti e le studentesse.

Quali sono gli interventi da mettere in atto in caso di "grooming"?

Casi di adescamento online richiedono l'intervento della **Polizia Postale e delle Comunicazio**ni a cui bisogna rivolgersi il prima possibile, tenendo sempre traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video…). L'adescamento, inoltre, può essere una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. **Consultorio Familiare**, **Servizio di Neuropsichiatria Infantile**, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.

I minori vittime di adescamento riferiscono, generalmente, di sentirsi traditi, ma anche di provare un senso di colpa per essere caduti in trappola ed essersi fidati di uno sconosciuto. Inutile sottolineare che nei casi più estremi in cui l'adescamento porta ad

un incontro fisico e ad un abuso sessuale un sostegno psicologico esperto per il minore è da considerarsi prioritario e urgente.

Per consigli e per un supporto è possibile rivolgersi alla **Helpline di Generazioni Connesse (19696)**: operatori esperti e preparati sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che dei bambini, degli adolescenti, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti l'utilizzo dei nuovi media

---

4.7 - Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, **concrete o simulate** o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

La legge n. 269 del 3 agosto 1998 *"Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella* ***legge n. 38 del 6 febbraio 2006*** *"Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet"*, segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

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

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile

parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione **"Segnala contenuti illegali"** (Hotline).

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

Gli studenti e le studentesse sono soggetti a rischio sia direttamente, in quanto possibili vittime di abusi a causa di sexting e grooming, sia in quanto coinvolti nella visione di questi contenuti.

Nel momento in cui ci si rende conto di un malessere psico-fisico di uno studente o di una studentessa sarà opportuno ricorrere a un supporto psicologico, anche passando per una consultazione presso il medico di base o pediatra di riferimento. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza: **Consultori Familiari**, **Servizi di Neuropsichiatria infantile**, **centri specializzati** sull'abuso e il maltrattamento all'infanzia, ecc.

Se si è a conoscenza di tale tipologia di reato, è possibile far riferimento ai seguentiservizi:

- Polizia di Stato – **Compartimento di Polizia postale e delle Comunicazioni**;
- Polizia di Stato – **Questura o Commissariato di P.S. del territorio di competenza**;
- Arma dei Carabinieri – **Comando Provinciale o Stazione del territorio di competenza**;
- Polizia di Stato – **Commissariato on line**.

Se casi di pedopornografia dovessero essere rilevati a scuola, ne sarà immediatamente informato il Dirigente Scolastico e verrà seguito l'iter di azione indicato nel capitolo seguente.

Facendo riferimento a quanto proposto da "Generazione Connesse" l'Istituto intende proporre un'attività di prevenzione che porti i più giovani ad acquisire competenze in grado di orientarli e guidarli nelle loro scelte on line; ecco perché è fondamentale un'attività di educazione all'affettività e alle relazioni, sottolineando sempre la necessità di rivolgersi ad un adulto quando qualcosa on line mette a disagio.

A seguire vengono descritte le azioni, rivolte a genitori, alunni e docenti, che il nostro

Istituto intende intraprendere per prevenire ed affrontare la delicata problematica della pedopornografia percorsi di riflessione e confronto proposti ai docenti e quindi agli studenti su questa tematica;:

- attività di sensibilizzazione degli alunni, che ricordino loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico: chi è immerso dalla nascita nelle nuove tecnologie spesso non è consapevole che una foto o un video diffusi in rete potrebbero non essere tolti mai più, né è sempre consapevole che scambiare o diffondere materiale pedopornografico sia un reato;
- inserimento nel curricolo, ove possibile, di temi legati all'affidabilità delle fonti on line e alla sessualità;
- informazione ai genitori circa le possibilità di attivare forme di controllo parentale della navigazione e sensibilizzazione sulla necessità di monitorare la presenza dei figli sui social e sulle chat.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2024/2025).

Scegliere almeno 1 di queste azioni:

☐ 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 informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.

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

Scegliere almeno 1 di queste azioni:

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

☐ 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.

☐ 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.

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).

È quindi essenziale, innanzitutto, che nelle procedure:

- si faccia riferimento a delle figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso;

- sia previsto il coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre che del Dirigente Scolastico.

Inoltre, a partire dalle risorse interne (ad esempio, docenti con competenze specifiche e formati sul tema, altre figure professionali presenti all'interno della scuola, come lo psicologo), la scuola potrà individuare le figure che costituiranno un team preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi, sarà importante prevedere 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. Sarà quindi importante coinvolgere e, se necessario, mettere a punto dei protocolli di collaborazione per definire un lavoro sinergico che si occupi sia dei risvolti giuridico-penali delle varie situazioni problematiche sia della sofferenza delle persone coinvolte.

Nella parte finale di questo modulo si propongono delle procedure standard di riferimento per le principali casistiche. Tali procedure dovranno successivamente essere 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 può avvenire 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.

Nelle Linee di orientamento per la prevenzione e il contrasto del cyberbullismo nel paragrafo 3.1. (pag. 9) si sottolinea come:

"le misure di intervento immediato che i Dirigenti Scolastici sono chiamati a effettuare, qualora vengano a conoscenza di episodi di cyberbullismo, dovranno essere integrate e previste nei Regolamenti di Istituto e nei Patti di corresponsabilità, al fine di meglio regolamentare l'insieme dei provvedimenti sia di natura disciplinare che di natura educativa e di prevenzione".

Procedure da attuare nel caso di

- **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 da 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, per quanto possibile, la rimozione del materiale (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.

E' possibile fare riferimento, 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.

L'Isis "Valceresio" promuove la sicurezza a scuola, luogo attento al benessere di chi lo vive e in cui le problematiche non vengono ignorate, ma gestite con una mobilitazione organizzata. Alla luce di questa premessa, la comunità scolastica tutta (docenti, genitori, studenti e studentesse, personale ATA) deve essere sensibile e deve agire con tempestività e responsabilmente nel caso sospetti o accerti che uno studente o una studentessa sia stato vittima o presunta vittima di casi di bullismo, cyberbullismo, adescamento on line, sexting e di altri cybercrimes.

Le procedure saranno condivise con l'intera comunità scolastica mediante:

- Gli organi collegiali deputati (il Collegio dei Docenti)
- il sito web della scuola assemblee dedicate rivolte a studenti e famiglie infografiche dislocate all'interno della scuola

Qui di seguito si ricordano alcuni rischi relativi al mondo virtuale che potrebbero – in molte circostanze – non essere percepiti come tali soprattutto dagli studenti e dalle studentesse, ma che invece devono essere segnalati secondo le procedure allegate a questa E-policy. E' dunque importante che la comunità educante (genitori, docenti, personale ATA), ma anche gli studenti e le studentesse, possano conoscerli, con l'obiettivo di prevenirli e, all'occorrenza, segnalarli.

- esposizione a contenuti ingannevoli e ad informazioni scorrette (fake news);
- esposizione a contenuti violenti, o uso di videogiochi diseducativi (gaming online, gioco d'azzardo online);
- esposizione a siti violenti, razzisti, inneggianti all'odio, che invitano al suicidio o a comportamenti alimentari scorretti (hate speech, siti pro-suicidio, siti proanoressia e pro-bulimia);
- contatti con adulti che vogliono conoscere e avvicinare ragazzi e ragazze (adescamento on line);
- molestie, vessazioni o maltrattamenti da coetanei mediante la rete, i social, le chat (cyberbullismo);
- scambio e/o diffusione non autorizzata di materiale a sfondo sessuale (sexting);

- uso eccessivo di Internet e dei device che mina la socialità (dipendenza);
- uso improprio di materiali personali – in particolare foto e video – (web reputation);
- uso scorretto dei device dell'Istituto (p.e. mediante il caricamento/l'apertura di programmi contenenti virus; installazione di software non autorizzati, senza licenza, non conformi alle leggi sul copyright).

In questo contesto si ribadisce l'importanza del fatto che i docenti, nell'espletamento delle loro funzioni di formatori ed educatori, sappiano cogliere ogni occasione per riflettere insieme agli alunni su tali rischi, anche ricorrendo all'aiuto di docenti che – in seno al Collegio –hanno un'adeguata formazione in merito. Fondamentale è poi monitorare con attenzione le relazioni all'interno della classe, onde poter individuare potenziali situazioni di disagio ed intervenire tempestivamente, anche mediante il ricorso alle figure specializzate, per sostenere il singolo nelle situazioni di difficoltà personale e indirizzare il gruppo verso l'instaurazione di un clima positivo, di reciproca accettazione e rispetto. Tale percorso interno potrà essere ulteriormente rinforzato dalla partecipazione a progetti e/o iniziative esterne coerenti con i temi sopramenzionati, cui la scuola porrà particolare attenzione, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità.

5.2. - Come segnalare: quali strumenti e a chi

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

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

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

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

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

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

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

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

Caso A

Avvisare il Referente d'Istituto per il contrasto del bullismo e del cyberbullismo valutando insieme le possibili strategie d'intervento. Si ritiene opportuno informare anche l'intero Consiglio di classe in quanto l'attenzione dei singoli docenti può essere meglio finalizzata ad un'osservazione delle dinamiche all'interno della classe; utile dunque un contatto – in questo frangente – costante tra i docenti del Consiglio di classe.

Se si ravvisano necessità e urgenza, può essere opportuno coinvolgere il Dirigente Scolastico. Nel frattempo il docente – preferibilmente alla presenza di un collega o del referente per il contrasto del bullismo e del cyberbullismo – ascolta gli studenti e le studentesse, osservando il clima della classe, le dinamiche relazionali e tiene traccia delle sue osservazioni e valutazioni.

E' fondamentale che il docente parli alla classe, senza particolari riferimenti al sospetto che nutre, ma invitando gli studenti e le studentesse a chiedere aiuto se pensano di vivere situazioni o di subire atti identificabili come bullismo e cyberbullismo. Questa modalità di azione può trovare spazio anche – e preferibilmente – all'interno di momenti laboratoriali, (gestiti dal docente, da un collega, dal referente per il contrasto del bullismo e del cyberbullismo) dedicati per esempio alla navigazione del sito di "Generazioni Connesse" o svolgendo con la classe altre attività che diano ai ragazzi e alle ragazze occasioni di riflessione anche personale, condivisa e informazioni su come agire per denunciare ciò cui potrebbero aver assistito, di cui

potrebbero aver sentito parlare. Stante la complessa e sempre diversa dinamica di situazioni analoghe a quella descritta, si ricorda che i docenti, gli studenti e le famiglie possono essere sempre supportati dalla Helpline del progetto Generazioni Connesse.

Caso B

Avvertire immediatamente il Referente per il contrasto al bullismo e cyberbullismo valutando insieme le possibili strategie d'intervento. Occorre coinvolgere il Dirigente Scolastico che convoca il Consiglio di classe in sessione straordinaria. Se non si ravvisano situazioni di reato si mettono in atto i seguenti ulteriori contatti:

- i genitori degli studenti o delle studentesse direttamente coinvolti, siano essi vittime, attori, spettatori; contestualmente si offriranno ai genitori informazioni per attuare la rimozione, l'oscuramento o il blocco di contenuti offensivi.
- lo psicologo scolastico per una consulenza di supporto all'azione della scuola ed eventualmente per supportare tutti o alcuni degli attori dell'evento;
- il Consiglio di classe che deve operare attivamente in sinergia perché la classe possa avere dei momenti di confronto e riflessione sulle tematiche legate all'evento.

A seconda della situazione e delle valutazioni effettuate con il referente, il Dirigente e i genitori, si può valutare un contatto con la Polizia Postale per segnalare il contenuto offensivo presente on line, la modalità di diffusione dello stesso e la fattispecie di reato eventuale. Parimenti è possibile prendere contatti con i servizi e le associazioni territoriali di riferimento (per esempio Consultorio che si occupa di problematiche adolescenziali, UONPIA o altro) nella necessità di un sostegno mirato. E' importante che di fronte ad atteggiamenti supposti o reali di bullismo e/o cyberbullismo, gli studenti e le studentesse siano educati a non essere omertosi (per paura di ritorsioni o vendette, per disinteresse, per non riconoscimento della gravità del fatto). Si ribadisce dunque la significatività di percorsi educativi in merito che devono essere sempre attivati anche alla luce di casi di cui si ha sospetto o che sono evidenti. Gli studenti e le studentesse sono parte attiva della relazione educativa.

Per aiutarli a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, l'Istituto prevede questi strumenti:

- indirizzo mail specifico (che verrà attivato e di cui verrà data accurata nota informativa) per le segnalazioni;
- box per la raccolta di segnalazioni anonime che verrà dislocato in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con lo psicologo scolastico;
- possibilità di rivolgersi, tramite mail istituzionale o di persona, al referente per il contrasto del bullismo e del cyberbullismo o ad altro docente di fiducia.
- Possibilità di rivolgersi alla Help line del progetto Generazioni Connesse, al numero gratuito 1.96.96

5.3. - Gli attori sul territorio

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

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

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

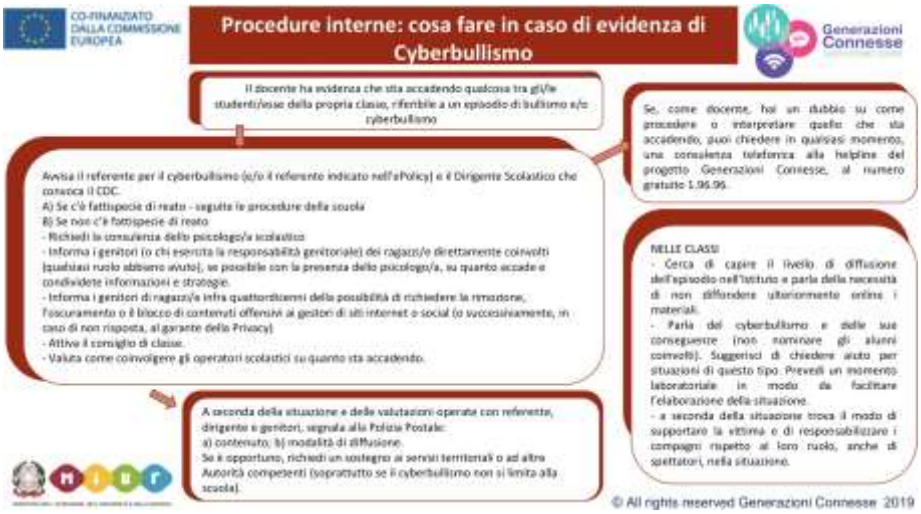
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

Si segnalano i seguenti servizi territoriali di possibile utilità:

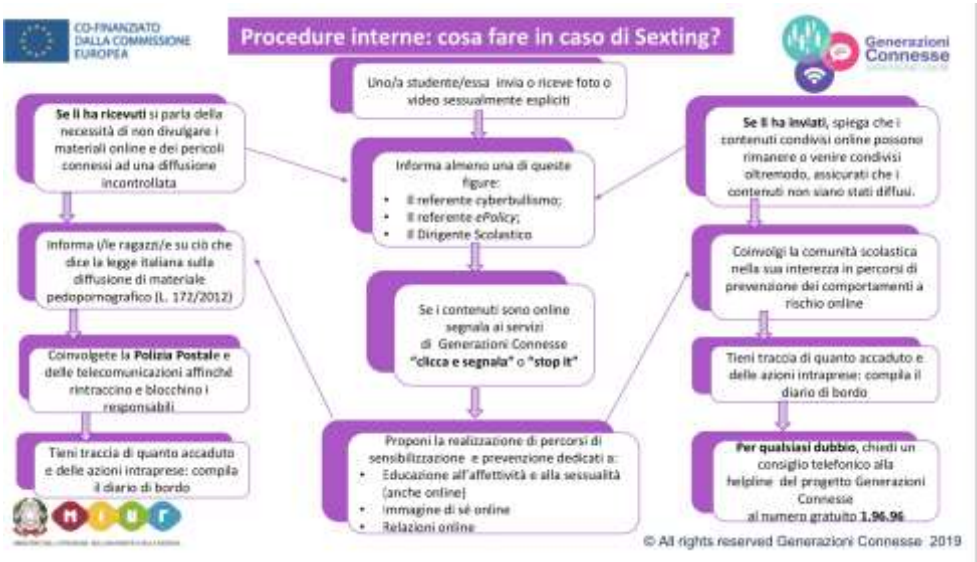
- **Co.Re.Com**: www.corecomlombardia.it, Sportello Help-Web Reputation Giovani; indirizzo: c/o Consiglio Regionale, Via F.Filzi, 22 20124 Milano; Contatti:02.67482725; corecomsegreteria@consiglio.regione.lombardia.it
- **Garante per l'Infanzia e l'Adolescenza**: Indirizzo: c/o Consiglio Regionale, Via F.Filzi, 22 20124 Milano; Contatti: 02.67486290; garanteinfanziaeadolescenza@consiglio.regione.lombardia.it
- **U S R** : www.usr.istruzione.lombardia.gov.it/aree-tematiche/bullismo-e-cyberbullismo
- **USP**: Via Copelli, 6, 21100 Varese; Contatti Tel. (+39) 0332 257 111; https://varese.istruzione.lombardia.gov.it/
- **Tribunale per i minorenn**i: www.trbmin.milano.giustizia.it Indirizzo: via Leopardi, 18 Milano; Contatti: 02.46721 tribmin.milano@giustizia.it
- **Polizia Postale e delle Comunicazion**i: Indirizzo: Viale Milano, 11, 21100 Varese VA, Contatti:0332 281402
- **ASL**: Indirizzo: Via O.Rossi, 9, 21100 Varese (VA), Contatti: 0332.277111, PEC protocollo@pec.ats-insubria.it, https://www.ats-insubria.it/
- **Comitato Unicef Varese**: Via Paolo Maspero, 20 21100 Varese, Contatti: 342 7560341, comitato.varese@unicef.it, https://www.unicef.it/comitati-locali/vares e/

5.4. - Allegati con le procedure

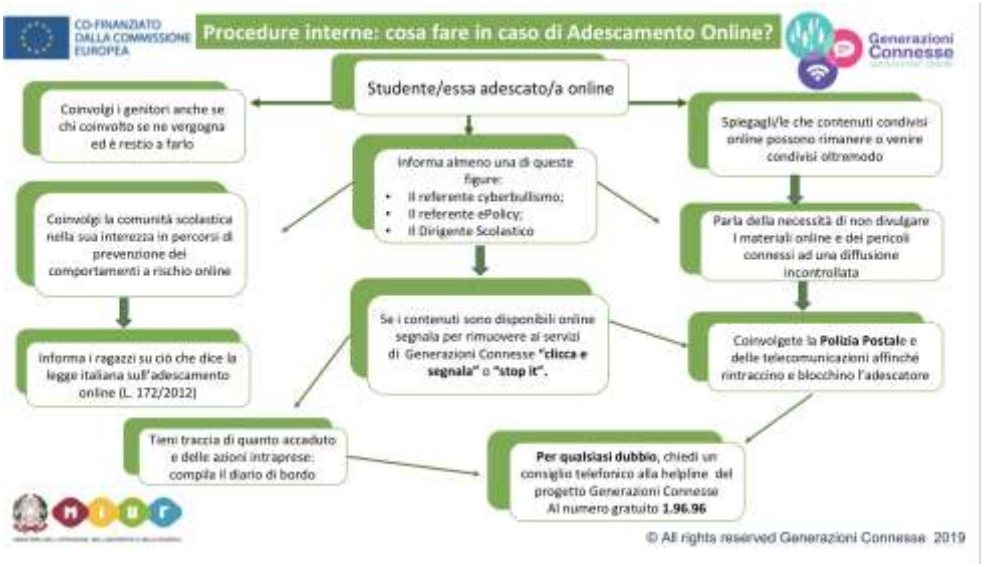
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



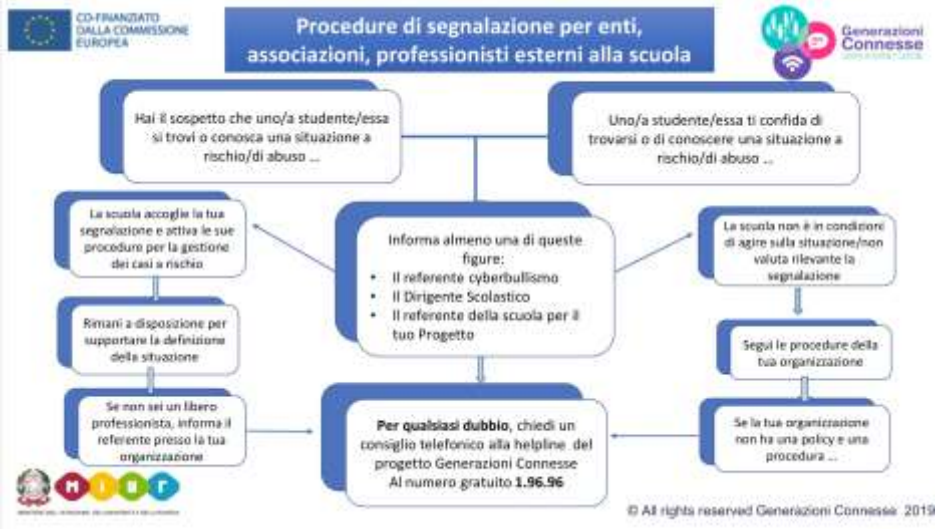
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

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

PROCEDURA INTERNA: COSA FARE IN CASO DI EVIDENZA DI CYBERBULLISMO

1. Il docente avvisa il Referente per il cyberbullismo e il DS
2. Il DS convoca il Consiglio di classe cui partecipa il Referente
3. Se emerge la fattispecie di reato, si applica il Regolamento d'Istituto
4. Se non emerge la fattispecie di reato:

- Il Referente per il cyberbullismo e il docente richiedono la consulenza dello psicologo scolastico;
- Il docente ed eventualmente anche il Referente informano i genitori di tutti i ragazzi direttamente coinvolti (qualsiasi ruolo abbiano avuto) su quanto accaduto; si condividono con loro informazioni e strategie.
- Il docente attiva il Consiglio di classe che decide come operare in sinergia e si confronta con il referente.
- Il docente, se ci sono i presupposti, può segnalare alla Polizia Postale contenuto e modalità di diffusione.
- Il docente, se il Consiglio di classe lo ritiene utile, può richiedere un sostegno ai servizi territoriali o ad altre Autorità competenti.

E' di fondamentale importanza che, alla luce del particolare evento verificatosi, ci sia una ricaduta educativa sull'intera classe attraverso per esempio percorsi, attività laboratoriali, discussioni che permettano di informare e sensibilizzare gli alunni in relazione alle problematiche emerse, ma senza fare riferimenti espliciti all'episodio e alle persone coinvolte. E' compito del Consiglio di classe elaborare tale strategia della cui realizzazione si occuperà almeno un docente con l'eventuale supporto del referente.

PROCEDURA INTERNA: COSA FARE IN CASO DI SOSPETTO DI CYBERBULLISMO

1. Il docente avvisa il Referente per il cyberbullismo e insieme a lui valuta possibili strategie d'intervento: possibilità di avvisare il Consiglio di classe (azione caldeggiata in quanto il confronto con gli altri docenti può contribuire a comprendere meglio la situazione) possibilità di avvisare il DS
2. Il docente interviene sulla classe sondandone il clima, ascoltando i ragazzi e monitorando ciò che accade senza entrare nello specifico del sospetto cercando, se possibile, anche di capire il livello di diffusione dell'episodio nell'Istituto.
3. Il docente interviene sulla classe, anche con l'eventuale collaborazione del

Referente, parlando del cyberbullismo, suggerendo di chiedere aiuto e fornendo agli studenti contatti quali help line di Telefono Azzurro.

4. Il docente si confronta con il Referente sull'iter seguito e sugli esiti ottenuti

PROCEDURA INTERNA: COSA FARE IN CASO DI SEXTING

Se uno studente o una studentessa invia o riceve foto o video sessualmente espliciti:

1. Informare il referente e il DS e concordare strategie di intervento
2. Informare i genitori e il Consiglio di classe
3. Se i contenuti sono on line, segnalare all'Help line di GC e contattare la Polizia Postale
4. Attivare almeno un percorso di sensibilizzazione e prevenzione dedicato all'educazione all'affettività/all'immagine di sé on line/alle relazioni on line

Se i contenuti sono stati ricevuti:

1. Ribadire la necessità di non divulgare questi materiali on line e i pericoli connessi ad una diffusione incontrollata
2. Informare sui contenuti della legge italiana in materia di diffusione di contenuti pedopornografici
3. Compilare il diario di bordo in relazione all'evento
4. Comunicare con il Referente

Se i contenuti sono stati inviati:

1. Spiegare che i contenuti condivisi on line possono rimanervi ed essere condivisi in modo incontrollato
2. Compilare il diario di bordo in relazione all'evento
3. Comunicare con il Referente

PROCEDURA INTERNA: COSA FARE IN CASO DI ADESCAMENTO ON LINE

Se uno studente o una studentessa viene adescato on line:

1. Informare il DS e il Referente e concordare strategie d'intervento (possibilmente con il supporto dello psicologo scolastico)
2. Informare i genitori
3. Contattare la Polizia Postale
4. Segnalare all'Help line di GC
5. Attivare almeno un percorso di prevenzione sui rischi on line

PROCEDURA DI SEGNALAZIONE PER ENTI, ASSOCIAZIONI, PROFESSIONISTI ESTERNI ALLA SCUOLA

Se il professionista ha il sospetto che uno studente o una studentessa si trovi in una situazione di rischio/abuso o ne sia a conoscenza:

1. Informa almeno una di queste figure: DS, Referente cyberbullismo, docente

referente della scuola per il progetto
2. L'Istituto prende in carico la segnalazione e attiva la procedura più adeguata

Se uno studente o una studentessa confida al professionista di trovarsi in una situazione di rischio/abuso o di esserne a conoscenza, il professionista:

1. Informa almeno una di queste figure: DS, Referente cyberbullismo, docente referente della scuola per il progetto
2. L'Istituto prende in carico la segnalazione e attiva la procedura più adeguata

Il nostro piano d'azioni

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