Documento di ePolicy

MBIS073006

IIS "LUIGI CASTIGLIONI"

VIA GARIBALDI115 - 20812 - LIMBIATE - MONZA E DELLA BRIANZA (MB)

Viviana Guidetti

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.

Il documento di E-policy stabilisce le procedure condivise che permettono di uniformare le azioni per sviluppare un corretto utilizzo delle TIC. Il documento sintetizza le indicazioni contenute nel Regolamento d'istituto, nel Piano della DDI, nel Patto di corresponsabilità.

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.

IL DIRIGENTE SCOLASTICO

Nel promuovere l'uso consentito delle tecnologie e di internet, il ruolo del Dirigente Scolastico è quello di:

- garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- garantire ai propri docenti una formazione di base sulle Tecnologie dell'Informazione e della Comunicazione (ICT) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse;
- garantire ai propri docenti una formazione di base sulle tematiche del bullismo e del cyberbullismo
- garantire l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza online;
- dover informare tempestivamente, qualora venga a conoscenza di atti di cyberbullismo, che non si configurino come reato, i genitori dei minori coinvolti (o chi ne esercita la responsabilità genitoriale o i tutori);
- regolare il comportamento degli studenti ed imporre sanzioni disciplinari in caso di comportamento inadeguato, in relazione all'utilizzo delle TIC.

L'ANIMATORE DIGITALE

L'Animatore digitale svolge i seguenti compiti:

- far pubblicare il documento E-policy sul sito della scuola;
- stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza ed informazioni al personale in relazione ai rischi online ed alle misure di prevenzione e gestione degli stessi;
- coinvolgere la comunità scolastica nelle azioni previste nel piano del PNSD;
- proporre soluzioni didattiche innovative e tecnologicamente sostenibili

ASSISTENTE TECNICO INFORMATICO

L'assistente tecnico informatico ha le seguenti responsabilità:

- promuovere la salvaguardia dei dati e la sicurezza della rete;
- tenere aggiornato il sistema operativo e i diversi software dei dispositivi fissi e mobili connessi in rete.

REFERENTE DEL CYBERBULLISMO

Il ruolo del Referente per Bullismo e Cyberbullismo include i seguenti compiti:

- coordina iniziative di prevenzione e contrasto del cyberbullismo messe in atto dalla scuola, anche avvalendosi della collaborazione delle Forze di Polizia, nonché delle associazioni e dei centri di aggregazione giovanile presenti sul territorio;
- costituisce l'interfaccia con le Forze di Polizia, con i servizi minorili dell'amministrazione della Giustizia, le associazioni ed i centri di aggregazione giovanile sul territorio, per il coordinamento delle iniziative di prevenzione e contrasto del cyberbullismo;
- svolge un importante compito di supporto al Dirigente, nonché all'Istituzione scolastica, per la revisione/stesura di Regolamenti, atti e documenti (PTOF, PdM, RAV, modello di e-policy d'Istituto);
- predispone documenti di rilevazione di incidenti di sicurezza in rete, attraverso la redazione di precisi format da protocollare;
- compila un prospetto per tenere traccia di eventuali segnalazioni (diario di bordo);
- promuove la conoscenza e la consapevolezza riguardo a bullismo e cyberbullismo, attraverso progetti d'Istituto che coinvolgano genitori, studenti e personale scolastico; facilita la formazione e la consulenza di tutto il personale;
- raccoglie e diffonde buone pratiche educative, organizzative e azioni di monitoraggio, anche attraverso la periodica somministrazione di questionari;
- collabora in team con altre figure scolastiche (Animatore Digitale e Team per l'Innovazione; Referente BES/Inclusione; Referente per la Dispersione);
- raccoglie le segnalazioni di casi di bullismi o cyberbullismo

I DOCENTI

Il ruolo del personale docente e di ogni figura educativa che lo affianca include i

seguenti compiti:

- provvedere personalmente alla propria formazione/aggiornamento sull'utilizzo del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in Internet e dell'immagine degli altri: lotta al cyberbullismo);
- supportare gli alunni nell'utilizzo consapevole delle tecnologie informatiche utilizzate a scopi didattici ed informarli/formarli sul divieto di plagio e sul rispetto della normativa vigente in merito ai diritti d'autore;
- segnalare al Dirigente scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazioni;
- supportare ed indirizzare alunni coinvolti in problematiche legate alla rete:
- segnalare sia al Dirigente scolastico che all'Animatore digitale e al Referente del cyberbullismo sia attraverso i canali istituzionali (in primo luogo il RE) qualsiasi violazione nell'utilizzo delle TIC e di Internet ed eventuali episodi di cyberbullismo;
- promuovere l'uso delle tecnologie digitali nella didattica integrando parti del curricolo della propria disciplina con approfondimenti ad hoc.

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO

Il Personale ATA è tenuto a:

- avere adeguata consapevolezza riguardo alle questioni di sicurezza informatica, alla politica d'Istituto e relative buone pratiche;
- segnalare qualsiasi abuso, anche solo sospetto, al Dirigente Scolastico e/o all'Animatore Digitale per le opportune indagini/azioni/sanzioni;
- provvedere personalmente alla propria formazione/aggiornamento sui rischi connessi all'utilizzo improprio del digitale con particolare riferimento alla dimensione etica (tutela della privacy, lotta al cyberbullismo).

GLI STUDENTI E LE STUDENTESSE

Il ruolo degli alunni prevede i seguenti compiti:

- avere consapevolezza delle situazioni di rischio legate alla rete, telefoni cellulari, fotocamere digitali;
- comprendere l'importanza di adottare buone pratiche di sicurezza online quando si usano le tecnologie;
- conoscere la politica della scuola sull'uso di dispositivi mobili e sull'uso delle immagini;
- adottare condotte rispettose degli altri anche durante la comunicazione in rete;
- comprendere l'importanza della segnalazione di ogni abuso, uso improprio, o accesso a materiali inappropriati, e conoscere il protocollo per tali segnalazioni;
- essere consapevoli del significato e della gravità di atti di cyberbullismo, a

tutela della propria ed altrui incolumità;
- assumersi la responsabilità di un eventuale utilizzo sbagliato delle tecnologie;
- partecipare attivamente a progetto che riguardano l'uso positivo delle TIC e della rete e farsi promotori di quanto appreso.

I GENITORI

I genitori e i tutori svolgono un ruolo cruciale nel garantire che gli studenti comprendano la necessità di utilizzare in modo sicuro, consapevole ed appropriato dispositivi digitali e mobili. Per tale scopo è necessario che essi:

- contribuiscano, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete e sull'uso responsabile dei device personali;
- incoraggino l'impiego delle TIC da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza;
- sostengano l'Istituzione scolastica nel promuovere le buone pratiche di e-safety;
- consultino periodicamente le sezioni del sito web a loro dedicate, in particolare il registro elettronico;
- agiscano in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite;
- rispondano per gli episodi commessi dai figli minori a titolo di culpa in educando (articolo 2048 del Codice civile). Infatti, sono esonerati da responsabilità solo se dimostrano di non aver potuto impedire il fatto. Ma nei casi più gravi per i giudici l'inadeguatezza dell'educazione impartita ai figli emerge dagli stessi episodi di bullismo, che per le loro modalità esecutive dimostrano maturità ed educazione carenti.

GLI ENTI EDUCATIVI ESTERNI E LE ASSOCIAZIONI

Gli enti educativi esterni e le associazioni che entrano in relazione con la scuola si conformano alla politica della stessa riguardo l'uso consapevole della rete e delle TIC, promuovono comportamenti sicuri, la sicurezza online e assicurano la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

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

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

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

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

I soggetti esterni che sono responsabili di iniziative educative e formative nell'istituto:

1. visionano e sottoscrivono l'informativa E-policy dell'istituto riguardo all'uso consapevole e responsabile della rete e delle TIC;
2. promuovono la sicurezza online durante l'attività di cui sono titolari;
3. segnalano ai docenti preposti e al dirigente scolastico eventuali comportamenti problematici o casi di abuso nell'uso della rete e delle TIC.

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.

Oltre alla pubblicazione del documento di E-policy sul sito web, l'Istituto prevede i seguenti interventi:

per i docenti:

- una delibera iniziale del documento di E-policy e una discussione collegiale in caso di aggiornamento;
- i nuovi docenti dell'Istituto visionano e sottoscrivono l'informativa E-policy riguardo all'uso consapevole e responsabile della rete e delle TIC;

per gli studenti:

- il coordinatore di classe (o altro docente incaricato dal CdC), in apertura di anno scolastico, comunica agli studenti la presenza del documento e il suo ruolo; si leggeranno alcuni passaggi significativi soprattutto relativi ai comportamenti da attuare in caso di bisogno (in particolare alla classi prime, in fase di accoglienza);

per le famiglie:

- la comunicazione avverrà al momento della sottoscrizione del Patto di corresponsabilità.

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.

Infrazioni degli alunni

Le principali infrazioni in cui è possibile che gli alunni incorrano a scuola utilizzando le TIC ed internet, messi a loro disposizione a fini puramente didattici, sono le seguenti:

- uso improprio della rete per esprimere giudizi, infastidire o impedire a qualcuno di esprimersi liberamente o partecipare al dialogo didattico-educativo;
- l'invio incauto o non autorizzato di immagini, foto o dati sensibili;
- la condivisione di immagini non appropriate, violente, intime o troppo spinte;
- la comunicazione incauta e non autorizzata con sconosciuti o soggetti comunque estranei all'azione didattico-educativa;
- il collegamento a siti web inappropriati durante attività laboratoriali di qualsiasi genere.

I provvedimenti disciplinari da adottare da parte dei consigli di classe nei confronti di alunni che abbiano commesso una o più infrazione alla policy, secondo quanto sopra, (in proporzione alla gravità dell'infrazione commessa) saranno i seguenti:

- richiamo verbale;
- nota sul Registro elettronico;
- sanzioni estemporanee commisurate alla gravità della violazione commessa
- assegnazione di attività aggiuntive di approfondimento da svolgere a casa

Nel caso in cui sia necessario sono convocati i genitori per un colloquio con i docenti e/o con il Dirigente scolastico.

A seconda del tipo di infrazione è possibile prevedere interventi di carattere educativo di rinforzo dei comportamenti corretti che riguardano tutta la classe.

Infrazione del Personale Scolastico

Le principali infrazioni in cui è possibile che il Personale scolastico incorra a scuola utilizzando le TIC ed internet sono le seguenti:

- utilizzo delle tecnologie e dei servizi della scuola per svolgere attività estranee all' insegnamento o al proprio profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- utilizzo delle comunicazioni elettroniche con genitori e/o alunni non compatibile con il proprio ruolo professionale;
- trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- diffusione delle password assegnate e custodia incauta dei device e delle credenziali di accesso, di cui potrebbero approfittare terzi;
- mancata o non attenta vigilanza degli studenti, che potrebbe favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- insufficiente azione di contrasto a terzi in situazioni critiche; di interventi correttivi o di sostegno a studenti;
- mancata segnalazione al Dirigente, all'Animatore Digitale di situazioni critiche rilevanti.

Il Dirigente Scolastico può controllare l'utilizzo delle TIC per verificarne la conformità

alle norme di sicurezza, compreso l'accesso ad internet e la posta elettronica inviata/pervenuta a scuola; procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone copia per eventuali successive investigazioni.

Tutto il personale è tenuto a collaborare con il Dirigente Scolastico ed a fornire ogni informazione utile alle valutazioni del caso ed all'avvio di procedimenti che possono avere carattere organizzativo-gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse.

Le infrazioni alla Policy possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e/o genitori a docenti e/o ATA. Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso.

Infrazioni dei genitori

Le principali infrazioni alla Policy in cui è possibile che i genitori o i tutori incorrano sono le seguenti:

- comunicazione a terzi delle credenziali di accesso personali al RE;
- utilizzo non corretto delle modalità di comunicazioni con la scuola;
- mancata vigilanza sul corretto utilizzo degli strumenti della scuola concessi in comodato d'uso.

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.

I documenti integrati con le norme contenute nell'E-policy sono raggiungibili sul sito della scuola al seguente indirizzo:

https://www.iiscastiglioni.edu.it/istituto/regolamenti/

1.7 - Monitoraggio

dell’implementazione della ePolicy e suo aggiornamento

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

Il monitoraggio dell’implementazione della policy avverrà all’inizio di ogni anno scolastico, contestualmente alla revisione del PTOF, a cura del Dirigente scolastico, del gruppo NIV, del Referente per il Bullismo e Cyberbullismo e dell’Animatore Digitale.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Presentazione al Collegio docenti del documento E-policy e sua delibera.
- Presentazione al Consiglio d'istituto del documento E-policy e sua delibera.
- Pubblicazione del documento E-policy sul sito web dell'Istituto

Azioni da svolgere nei prossimi 3 anni:

- Integrazione del documento di E-policy con il Regolamento d'Istituto, il Regolamento di disciplina, il Patto di corresponsabilità e il Piano della DDI
- Fornire ai nuovi docenti della scuola il documento E-policy.
- Proporre assemblee di classe per la presentazione e discussione del documento E-policy.

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.

Tale curricolo digitale interesserà tutte le classi e tutti gli indirizzi e verterà sui temi della cittadinanza digitale e dell'uso sicuro e consapevole della rete. Il percorso verrà progettato e realizzato da docenti interni alla scuola, con lo specifico supporto dei docenti facenti parte della commissione E-policy, eventualmente avvalendosi di professionisti esterni con cui sviluppare alcune tematiche sul bullismo, cyberbullismo e reati digitali, utilizzo sicuro della rete, utilizzo dei dati personali in rete, netiquette, diritto all'informazione in rete, fake news, hate speech. La competenza digitale è annoverata tra i saperi necessari per la cittadinanza.

La competenza digitale si basa su:

- la dimensione tecnologica che fa riferimento a una serie di skills di base ma anche a livelli più avanzati che riguardano la capacità di valutare e selezionare quali strumenti tecnologici digitali possono risolvere uno specifico problema;

- la dimensione cognitiva che fa riferimento alle abilità legate al trattamento dell'informazione, dalla capacità di accedere, selezionare e interpretare i dati a quella di valutarne la pertinenza e l'affidabilità;
- la dimensione etica e sociale, la prima fa riferimento alla capacità di gestire in modo sicuro i propri dati personali e quelli altrui e di usare le tecnologie digitali per scopi eticamente accettabili, nel rispetto degli altri; la seconda riguarda le abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di coloro con cui comunichiamo online.

Dalla integrazione di queste tre principali dimensioni emerge un concetto di competenza digitale che fa riferimento alla capacità di comprendere e sfruttare l'effettivo potenziale delle tecnologie in una ottica di costruzione, di conoscenza e di promozione della partecipazione e dell'inclusione.

In sintesi l'istituto attiverà un percorso così strutturato:

Aree di competenza

- **Informazione**

  Descrittore:

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

- **Comunicazione**

  Descrittore:

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

- **Creazione di contenuti**

  Descrittore:

  - Lo studente realizza e modifica contenuti (da elaborazione testi a immagini e video); integra e rielabora conoscenze, produce contenuti in

modo creativo

- **Problem-Solving**

  Descrittore:

  - Lo studente utilizza gli strumenti digitali per identificare e risolvere piccoli problemi tecnici, contribuisce alla creazione di conoscenza, produce risultati creativi ed innovativi, supporta gli altri nell'uso degli strumenti digitali

- **Sicurezza**

  Descrittore:

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

Strumenti

- Rete e connettività
- Registro elettronico e ambiente di lavoro condiviso
- Google Work Space for Education (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, verifiche formative e sommative, 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...)
- Software per la didattica collaborativa (es. Padlet, Google Maps, Etwinning, Pik-to-chart, Storyboard that, Speak-Pic...)
- Software per lo sviluppo del pensiero computazionale e il making educativo (es. coding, Ultimaker Cura, pacchetto Autodesk...)
- Software per la realizzazione di mappe concettuali (es. CMap...) e video tutorial (es. Premiere, Windows media player, Powtoon...)
- Software per videoconferenza (Meet, GoToMeeting, Zoom...)

Traguardi formativi

- Utilizzare la rete per scopi di informazione, comunicazione, ricerca e svago
- Utilizzare strumenti informatici e di comunicazione per elaborare dati, testi e

immagini e produrre documenti
- Conoscere le caratteristiche e le potenzialità tecnologiche degli strumenti d'uso più comuni (PC, tablet, smartphone, strumenti di archiviazione e memoria digitale)
- Riconoscere vantaggi, potenzialità, limiti e rischi connessi all'uso delle tecnologie più comuni, anche informatiche
- Apprendere e utilizzare gli "aggregatori" digitali
- Cogliere e sfruttare le potenzialità creative e non solo quelle funzionali delle applicazioni digitali
- Apprendere come discriminare le fonti di informazione più affidabili

La scuola si impegna a condurre percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali.

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.

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

Al fine di promuovere la condivisione di buone pratiche per un uso consapevole e sicuro delle TIC e di prevenire e contrastare "ogni forma di discriminazione e del bullismo, anche informatico" (Legge 107/2015, art. 1, c. 7, l), l'Istituto attiverà un

piano d'azione che ha lo scopo di:

- analizzare il fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica;
- promuovere la partecipazione del corpo docente ai corsi di formazione sull'utilizzo e l'integrazione delle TIC nella didattica;
- organizzare incontri con esperti;
- fornire formazione istituzionale in contrasto al bullismo e al cyberbullismo attraverso gli snodi formativi del Ministero dell'Istruzione;
- formazione specifica di Istituto, legata alle esigenze formative rilevate.

Il corpo docente ha potuto partecipare a corsi di formazione, anche nell'ambito di Piani Nazionali, a momenti di autoaggiornamento e momenti di formazione personale o collettiva anche all'interno dell'Istituto, con la condivisione delle conoscenze dei singoli e il supporto dell'Animatore digitale. Possiede generalmente una buona competenza di base e, nel caso di alcune figure (Animatore digitale e Team), anche di carattere specialistico. È inoltre disponibile ad aggiornarsi, in quanto il percorso complesso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica è un processo in continua evoluzione.

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 regolare, 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.

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.

L'Istituto, attraverso il sito scolastico darà ampia diffusione del presente documento di E-policy per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e favorire un'attiva collaborazione tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi ad un uso non consapevole e critico del digitale, inoltre s'impegna a condividere materiali dedicati agli alunni e alle famiglie come guide in formato pdf e video, che possono fornire spunti di approfondimento.

Allo scopo di mantenere viva l'attenzione delle famiglie sull'uso consapevole delle TIC, della rete e delle numerose situazioni di rischio online, l'Istituto promuoverà opportunità di incontro e formazione per le famiglie sui temi oggetto della E-policy, offerte dal territorio, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità e la diffusione di materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati e dalle forze dell'ordine. Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i giovani nelle chat line o nei social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo. Inoltre, al fine di valorizzare e far conoscere alle famiglie il contributo degli studenti, l'Istituto predisporrà una sezione online dove sarà possibile pubblicare i progetti realizzati dagli studenti della scuola nella giornata mondiale della sicurezza in rete. In considerazione

dell'importanza di favorire la sinergia degli interventi educativi di scuola e famiglia per il successo scolastico ed educativo di ogni studente, il presente documento va ad integrare il Patto di Corresponsabilità.

Il nostro piano d'azioni

PeAzioni (da sviluppare nell'arco dell'anno scolastico 2021/2022)

- 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.

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

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

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

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.

La nostra scuola garantisce la tutela della privacy degli utenti attraverso l'applicazione del regolamento d'Istituto e del patto di corresponsabilità.

Il personale scolastico è responsabile del trattamento dei dati personali nei limiti delle operazioni e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Tutto il personale incaricato riceve istruzioni in merito al trattamento di dati personali ai fini della protezione e sicurezza degli stessi. In caso di attività di ampliamento dell'offerta formativa, organizzate in collaborazione con Enti esterni, viene richiesto preventivamente ai genitori il consenso informato alle riprese audio/ video e al loro eventuale utilizzo per scopi didattici, informativi e divulgativi anche tramite pubblicazione su siti web.

In relazione al nuovo 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), per agevolare l'applicazione del GDPR, l'Istituto ha provveduto alla nomina del Dott. Ing. Antonio Bove. Il titolare del trattamento dei dati è il Dirigente scolastico Dott.ssa Viviana Guidetti.

3.2 - Accesso ad Internet

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

> *di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

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

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

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

L'istituto è dotato di una strumentazione tecnologica attiva in modo capillare in tutti gli spazi. La connettività alla rete è garantita dalla fibra ottica in modalità via cavo e Wi-Fi ed offre la connessione ad internet per le attività sia didattiche sia amministrative. La rete della segreteria è separata dalla rete didattica e, grazie ad un diverso canale del medesimo firewall e ad un server dedicato, gestisce in modo autonomo e con regole differenti la sicurezza. Il Dirigente Scolastico, il corpo docente, il Direttore dei Servizi Generali e Amministrativi, il personale degli uffici della segreteria accedono ai servizi tramite procedura di autenticazione personale che prevede l'utilizzo di password aventi caratteristiche adeguate. La rete didattica, dotata di firewall dedicato, fornisce in sicurezza la connessione alle 36 classi provviste di strumentazione tecnologica, ai laboratori scientifici, multimediali, alla biblioteca e alle aule multifunzionali destinate al lavoro dei docenti. Il firewall non permette l'accesso ai siti non attendibili. In tutti questi spazi l'utilizzo quotidiano del registro elettronico è gestito da Axios che ne garantisce la protezione dei dati, così come la normativa richiede. L'accesso alla strumentazione e alla connessione è consentito ai docenti solo ai fini didattici ed è normato da password gestite dal responsabile della rete dell'Istituto e dagli assistenti tecnici informatici. Gli studenti accedono alla rete sotto il controllo dei docenti e degli assitenti durante le attività didattiche. Gli assistenti tecnici informatici hanno cura di aggiornare periodicamente il software e il

sistema operativo a garanzia della protezione da aggressioni esterne e dalle vulnerabilità che emergono nel tempo.

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.

Relativamente agli ambienti di apprendimento, il nostro Istituto si avvale di:

- sette laboratori con collegamento a Internet, tra cui un laboratorio linguistico;
- due laboratori di informatica;
- una biblioteca dotata di LIM/Smart TV;
- un'aula multifunzione multimediale;
- centotrentotto PC e Tablet presenti nei laboratori;
- due LIM/Smart TV presenti nei laboratori;
- quarantuno LIM - Una per ogni aula
- gli studenti e le studentesse sono dotati di dispositivi mobili, di proprietà, sui quali vengono scaricati i libri di testo in formato digitale e che, inoltre, offrono l'opportunità di instaurare un'interazione innovativa tra discenti e docenti attraverso l'uso di determinati web tool che consentono un utilizzo più agevole, costante e sistematico della piattaforma E-Twinning finalizzata alla costruzione di gemellaggi elettronici con diverse scuole Europee.

Riguardo agli strumenti di comunicazione esterna, il nostro istituto utilizza:

- il sito web - https://www.iiscastiglioni.edu.it/, costantemente aggiornato e i social network – Pagine Facebook e Istangram.

Per la comunicazione interna vengono utilizzati:

- il registro elettronico, che consente di gestire in modo ottimale la comunicazione con le famiglie che hanno la possibilità di essere costantemente informate interagendo direttamente con la scuola;
- la mail scolastica;
- app e piattaforme che hanno favorito un lavoro collaborativo e condiviso rendendo possibile un agevole passaggio alla didattica a distanza nel periodo di lockdown.

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.

Il nostro Istituto si è dotato di una regolamentazione condivisa e specifica su tali aspetti. Nel Patto di Corresponsabilità condiviso con le famiglie e dalle stesse sottoscritto a inizio anno, relativamente all'uso dei telefoni cellulari, viene chiaramente specificato che:

l'utilizzo del telefono cellulare durante l'attività scolastica è regolamentato anzitutto:

- dal D.P.R. 24 giugno 1998, n. 249, "Regolamento recante lo Statuto delle studentesse e degli studenti";
- dalla C. M. 25 agosto 1998, n. 362, "Uso del telefono cellulare nelle scuole";
- dal D.M. 15 marzo 2007, n. 30, "Linee di indirizzo ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, dovere di vigilanza e di corresponsabilità dei genitori e dei docenti";
- dal D.M. 30 novembre 2007, n. 104, "Linee di indirizzo e chiarimenti sulla normativa vigente sull'uso di telefoni cellulari e di altri dispositivi elettronici nelle comunità scolastiche";
- dai "Dieci punti per l'uso dei dispositivi mobili a scuola" pubblicati dal Ministero il 19 gennaio 2018.

In, particolare, è vietato utilizzare il telefono cellulare e altri dispositivi elettronici e di intrattenimento (tablet, notebook, fotocamera, videocamera, casse, ecc.) durante le attività didattiche in aula e in tutti i locali della scuola, nel rispetto di quanto sancito dal D.P.R. n. 249/1998. Il divieto risponde a una generale norma di correttezza, in quanto l'utilizzo del telefono cellulare o di altri dispositivi elettronici rappresenta un elemento di distrazione sia per chi lo usa sia per il resto della classe, oltre che una grave mancanza di rispetto. La violazione di tale divieto configura un'infrazione disciplinare rispetto alla quale la scuola è tenuta ad applicare apposite sanzioni ispirate al criterio di gradualità e alle finalità educative della scuola, per le quali si rimanda al Regolamento di disciplina. Gli studenti che hanno con sé i predetti dispositivi devono tenerli spenti e opportunamente custoditi e depositati nei borsoni, zaini, giacconi o armadietti personali. In casi eccezionali, qualora il Consiglio di classe ritenga che l'uso improprio del telefono cellulare sia un comportamento generalizzato all'interno della classe, i docenti possono chiedere agli studenti il deposito in un apposito contenitore dei propri dispositivi. Gli studenti avranno cura di proteggere i dispositivi da eventuali danni causati dal contatto con gli altri dispositivi. I docenti non saranno responsabili di eventuali danni riscontrati sui dispositivi al termine delle lezioni. Durante le ore di lezione eventuali gravi e urgenti esigenze di comunicazione tra gli studenti e le famiglie potranno essere soddisfatte, come è sempre avvenuto, mediante gli uffici di presidenza e di segreteria amministrativa; in alternativa, il docente potrà concedere l'autorizzazione all'uso del cellulare, previa richiesta motivata da parte dello studente. All'interno di tutti i locali della scuola, nelle sedi utilizzate per l'attività didattica come palestre, aule e laboratori sono vietate riprese fotografiche, audio e video di ambienti e persone, salvo in caso di un utilizzo per fini didattici. È sempre esclusa la possibilità di pubblicazione e diffusione del materiale prodotto. Eventuali riprese fotografiche, audio e video improprie si configurano come violazione della privacy e quindi perseguibili per legge. Il divieto di utilizzare il cellulare è da intendersi rivolto anche al personale della scuola. É comunque fatta salva la possibilità per i docenti di utilizzare dispositivi elettronici personali per tutte le operazioni inerenti la gestione del Registro di classe. **È consentito ai docenti di organizzare**

la propria attività didattica mediante utilizzo dei diversi dispositivi elettronici, anche da parte degli studenti, qualora lo si ritenga funzionale all'attività stessa.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022).

- Organizzare un evento o un' attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali e/o sulla cybersecurity
- Organizzare un evento o un'attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali e/o sulla cybersecurity

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

Scegliere almeno 1 di queste azioni:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse;
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali;

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.*

Le fasi attuative dal punto di vista operativo si possono declinare come segue:

1. Programmare degli interventi mirati, con l'ausilio di eventuali esperti esterni in materia, dove si analizzano determinate problematiche o condizioni
2. Raccogliere il feed-back da parte degli studenti

Nel caso della prevenzione si distinguono tre tipi di prevenzione:

1) Quella universale presuppone che tutti gli studenti siano potenzialmente a rischio, quindi si rivolge ad un grande pubblico

2) Quella selettiva che si rivolge ad un gruppo scelto in base a precedenti indagini e segnalazioni

3) Quella indicata che consiste in un intervento su caso specifico. In questo ultimo caso risulta opportuno coinvolgere anche la famiglia

L'istituto metterà a disposizione una scheda di segnalazione accessibile al personale docente e un modulo/mail per gli studenti al fine di permettere loro di segnalare/denunciare, in piena riservatezza, una situazione di bisogno.

L'istituto favorisce la raccolta ed utilizzo di materiale esplicativo uniformato e condiviso per agevolare e armonizzare le azioni di prevenzione.

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).

L'istituto agirà su due fronti:

PREVENZIONE

- formazione del personale scolastico e lo sviluppo di competenze digitali, non solo nei docenti ma anche negli studenti
- incontri di formazione con l'ausilio delle forze dell'ordine, delle associazioni di supporto psicologico che operano nella scuola e delle associazioni presenti sul territorio.
- programmazione di lezioni mirate a scopo formativo, in discipline che si prestano alla trattazione di queste tematiche;

AZIONE

- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;

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.

AZIONI

- favorire un dialogo consapevole e costruttivo tra studenti e corpo docente
- il coordinatore di classe, una volta ventuto a conoscenza di una problematica, si attiva per mettere in atto le seguenti azioni:
    - Contatto con il referente Cyberbullismo e/o il Dirigente scolatico
    - Individuazione di strategie da mettere in atto (con eventuali sanzioni)
    - Eventuale coinvolgimento del Consiglio di Classe
    - Valutazione finale dell'efficacia dell'intervento

4.4 - Dipendenza da Internet e gioco online

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

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

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso riflessioni sul benessere Digitale mediante questo percorso privilegiato:

- Presa di coscienza da parte degli studenti dei confini del benessere digitale mediante l'attivazione di un dibattito guidato che verta sulle seguenti tematiche:

- Come trascorri il tempo on line?
- Quando aggiunge valore alla tua vita e quando ti fa perdere tempo?
- Quale atteggiamento potresti cambiare quando sei online?
- Che ruolo ha e deve avere la tecnologia (internet o il gioco) nella tua vita?

In presenza di veri e propri fenomeni di dipendenza, il consiglio di classe valuterà se coinvolgere le associazioni di supporto psicologico che operano nella scuola

---

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.

Il sexting (abbreviazione di sex – sesso e texting – messaggiare, inviare messaggi) indica l’invio e/o la ricezione di contenuti (video o immagini) sessualmente espliciti che ritraggono se stessi o gli altri e che vengono diffusi attraverso siti, e mail, chat. L'invio di foto che ritraggono minorenni al di sotto dei 18 anni in pose sessualmente espicite configura, infatti, il reato di distribuzione di materiale pedo-pornografico.

L’istituto promuove azioni di sensibilizzazione e prevenzione sopracitate anche relativamente a questo argomento.

4.6 - Adescamento online

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

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di

instant messaging (whatsapp, telegram etc.), i siti e le app di ***teen dating*** (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

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

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

L'istituto promuove le azioni di sensibilizzazione e prevenzione anche relativamente a questo argomento, in modo particolare rivolto agli studenti del biennio.

Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e perché no, della sessualità.

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.

L'istituto promuove le azioni di sensibilizzazione e prevenzione anche relativamente a questo argomento, in modo particolare rivolto agli studenti del biennio.

Vedasi paragrafo 4.6

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022).

Verrà attivata una delle seguenti azioni:

☐ Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

☐ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

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

☐ Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

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

Verrà attivata una delle seguenti azioni:

☐ Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

☐ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

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

☐ Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

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

segnalare la presenza di materiale pedopornografico online.

Si considerano da segnalare tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni che mirano a insultare, minacciare, diffamare e/o ferire una persona (o un piccolo gruppo) tramite un utilizzo irresponsabile delle TIC. In particolare si segnaleranno:

- contenuti che violano la privacy;
- contenuti aggressivi o violenti;
- contenuti di natura sessuale.

Tutte le segnalazioni riportate dai docenti verranno registrate su apposita scheda.

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.

Le segnalazioni possono essere inviate a:

sos@iiscastiglioni.edu.it;

sportello di ascolto: cantiere@iiscastiglioni.edu.it;

docenti referenti:

Dirigente scolastico prof.ssa Viviana Guidetti

Referente Cyberbullismo prof. Davide Maggi

Animatore Digitale prof.ssa Maria Luisa Croci

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.

Comitato Regionale Unicef: 024654771 comitato.lombardia@unicef.it

per Monza e della Brianza 039380680 comitato.monza@unicef.it

Co.Re.Com 0267482433 corecom.segreteria@consiglio.regione.lombardia.it

Ufficio scolastico regionale: Regione Lombardia: 025746271 drlo.urp@istruzione.it

Polizia postale e delle comunicazioni: 0243333011
https://www.commissariatodips.it/segnalazioni/segnala-online/index.html

Azienda sanitaria locale: 02994308642

Rete dei servizi per le dipendenze: Fondazione Eris convenzionata con SSN 0283241125 segreteria@fondazioneeris.it

Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico: 0267482736

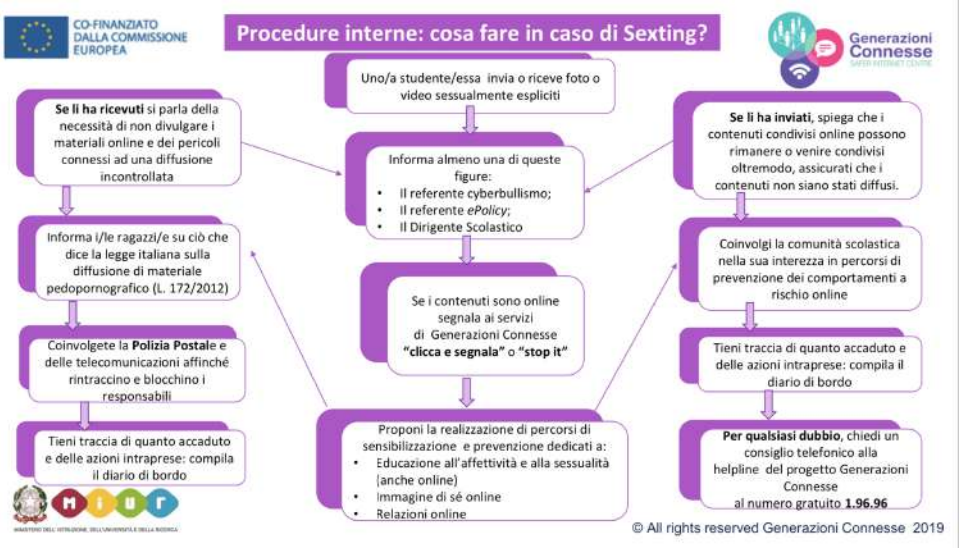
garanteinfanziaeadolescenza@pec.consiglio.regione.lombardia.it

Tribunale per i minorenni: 0246721 min.milano@giustizia.it

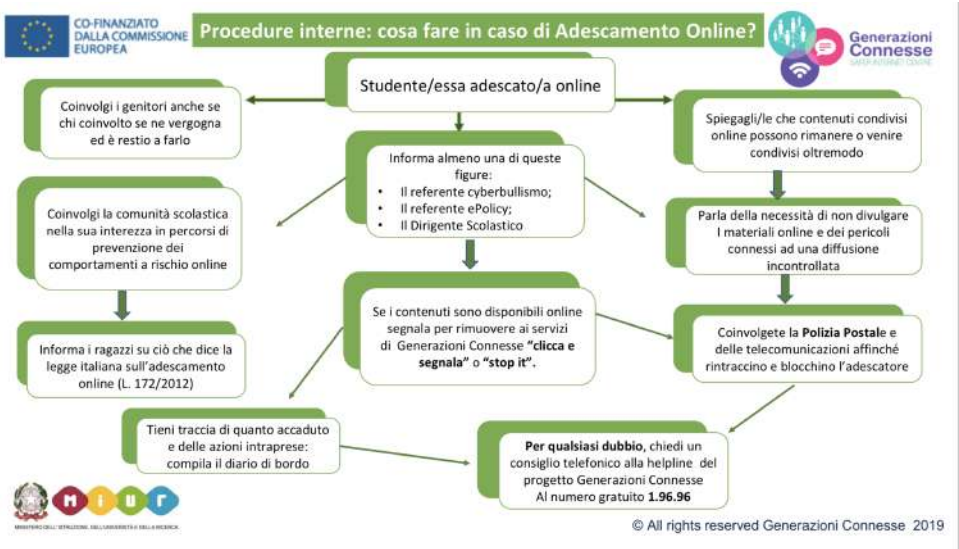
5.4. - Allegati con le procedure

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

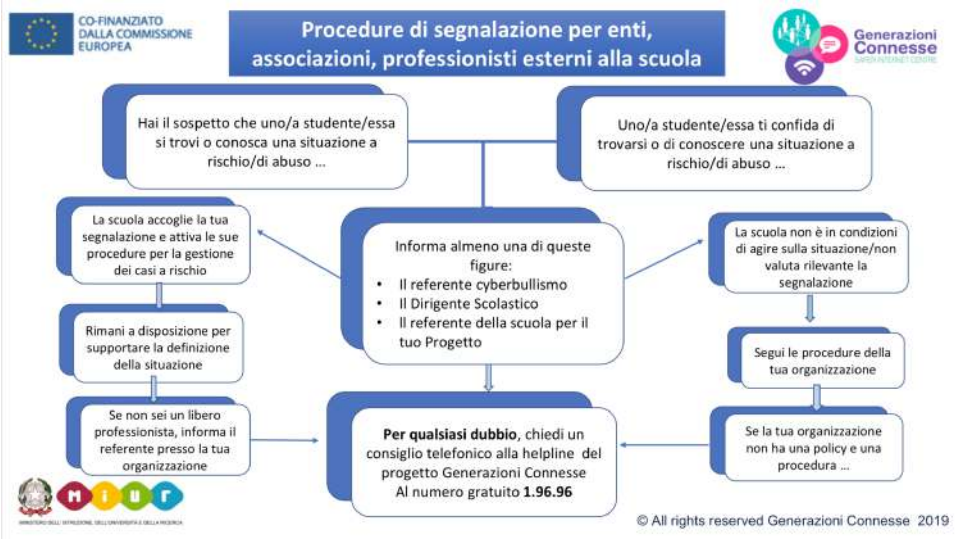
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Il nostro piano d'azioni

.