# Documento di ePolicy

ORIS00800B

I.I.S. "G. A. PISCHEDDA"

VIALE ALGHERO - 08013 - BOSA - ORISTANO (OR)

Rosella Uda

# 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.

# 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.

**La Dirigente Scolastica**

1. Garantisce la formazione del personale docente e non docente sulla sicurezza e sulla prevenzione on-line;
2. Controlla e vigila su fenomeni di hacking ai danni delle reti e dei computer dell'Istituto, nonché delle piattaforme utilizzate per la didattica e, per la gestione dei dati amministrativi, promuove la cultura della sicurezza on-line favorendo iniziative di formazione e prevenzione del fenomeno del cyberbullismo;
3. Ha la responsabilità di intervenire nei casi più gravi di bullismo, cyberbullismo e uso improprio delle tecnologie digitali.

**L'Animatore Digitale e il team digitale**

1. Offrono, se necessario, alla comunità scolastica il proprio supporto per quanto concerne gli aspetti tecnico-informatici;
2. Promuovono percorsi di formazione interna per la scuola al fine di garantire lo sviluppo delle competenze digitali;
3. Sono coinvolti nelle attività di formazione e di autoformazione in tema di uso responsabile della rete;
4. Promuovono l'adesione ai bandi relativi allo sviluppo delle competenze digitali;
5. Rilevano le problematiche connesse all'utilizzo delle TIC;
6. Supportano, se necessario, le attività del personale tecnico e amministrativo in relazione all'utilizzo delle tecnologie informatiche;
7. Interagiscono e cooperano con la DS, con la DSGA, con le Funzioni Strumentali d'Istituto e con il referente interno per il sito Web per le tematiche di sua competenza.

**Il Referente bullismo e cyberbullismo**

1. Coordina e promuove iniziative specifiche per la prevenzione e il contrasto del

bullismo e del cyberbullismo, avvalendosi della cooperazione delle forze di Polizia e Carabinieri, degli psicologi operanti presso la scuola, delle associazioni operanti nel territorio;
2. Coinvolge nei percorsi di formazione tutte le componenti della comunità scolastica: personale docente e non docente, studenti, genitori.

**I Docenti**

1. Integrano il curriculum delle proprie discipline promuovendo l'uso delle TIC, nel rispetto della libertà d'insegnamento;
2. Accompagnano e supportano gli studenti nelle attività di apprendimento nelle aule e nei laboratori dotati di LIM, monitor interattivi o di altri dispositivi;
3. Favoriscono la dematerializzazione delle attività relative alla didattica;
4. Segnalano, in quanto Pubblici Ufficiali, alla Dirigente Scolastica eventuali problematiche o casi di violenza e abuso on-line in cui siano coinvolti gli studenti, nel momento in cui ne vengano a conoscenza.

Gli Assistenti Tecnico - Informatici

1. Garantiscono supporto tecnico a studenti e docenti nelle aule e nei laboratori che prevedono l'uso della LIM e di altri dispositivi;
2. Segnalano, in qualità di Incaricati di Pubblico Servizio, comportamenti non adeguati nell'uso delle TIC ed episodi di bullismo e di cyberbullismo, nel momento in cui ne vengano a conoscenza;
3. Fanno sì che gli utenti autorizzati accedano alla rete della scuola tramite password;
4. Favoriscono l'informatizzazione di parte delle comunicazioni scuola-famiglia.

**Gli Studenti e le Studentesse**

1. Utilizzano le tecnologie digitali all'interno di percorsi formativi coerenti con gli obiettivi didattici ed educativi definiti dal Collegio Docenti;
2. Imparano a tutelare se stessi e i propri compagni dai rischi on-line;
3. Partecipano con senso di responsabilità alle iniziative e ai progetti di formazione proposti dalla scuola circa l'uso della rete e delle TIC.

**I Genitori**

1. Si impegnano a relazionarsi in maniera costruttiva con i docenti e ad agire in continuità con l'Istituto scolastico nella promozione e nell'educazione dei propri figli all'uso consapevole delle TIC e della rete, nonché all'uso corretto e responsabile dei device personali;
2. Controllano e vigilano costantemente sulle attività svolte dai propri figli sui social network;
3. Leggono, accettano e condividono, all'atto dell'iscrizione, la E-policy

dell'Istituto.

---

# 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).

Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, relativamente all'utilizzo 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. Prendono visione della politica dell'Istituto riguardo l'uso consapevole e responsabile della rete e delle TIC;
2. Promuovono la sicurezza on-line durante le attività di cui sono titolari;
3. Segnalano ai docenti preposti e alla Dirigente Scolastica 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.

## 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.

## 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.

Si indicano alcune proposte di modifica e/o integrazione del Regolamento di Disciplina, da definire e approvare nelle sedi opportune.

Integrazione del primo capoverso:

Visto l'art. 3 del DPR 249/98 e successive modifiche di cui al DPR 235/2007 e la nota prot. 3602/PO del 31 Luglio 2008 (Statuto degli studenti e delle studentesse e successive modifiche);

vista la Legge 547/93 (modificazioni e integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica);

visto il D.P.R. 390/90 e sue successive modifiche (T.U. delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza);

vista l'e-Policy d'Istituto;

visti i Regolamenti interni d'Istituto relativi al divieto di fumo e all'uso dei laboratori, della biblioteca, degli impianti sportivi, della palestra;

si individuano i comportamenti che si configurano come mancanze disciplinari:

- mancato rispetto dell'identità e dell'orientamento sessuale degli studenti e del personale scolastico.
- qualsiasi atto ascrivibile a bullismo, cyberbullismo, sexting, pedopornografia.
- qualsiasi azione di hacking ai danni del registro elettronico e/o del sito della scuola (violazione e/o diffusione delle credenziali, alterazione, danneggiamento, cancellazione di dati o software…), anche ai fini della falsificazione.
- qualsiasi azione di hacking ai danni delle reti d'istituto (violazione e/o diffusione delle credenziali, alterazione, danneggiamento, uso delle reti per scopi o attività sanzionate dalla legge o comunque non previste dai Regolamenti specifici).
- qualsiasi azione di danneggiamento di hardware, periferiche e software delle apparecchiature informatiche dell'Istituto.
- mancato rispetto dei vincoli d'uso e restituzione degli strumenti, anche informatici, dati in comodato d'uso agli studenti.

---

# *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 nostro piano d'azioni*

Azioni da svolgere entro un'annualità scolastica:

- Creazione del gruppo di lavoro E-policy, così costituito: referenti per la prevenzione del bullismo e del cyberbullismo, Team antibullismo e Team per l'emergenza, F.S. "Aggiornamento del PTOF, monitoraggio, valutazione e autovalutazione del PTOF, dei percorsi didattici e del servizio scolastico", F.S. "Sostegno al lavoro docente e Gestione e coordinamento del settore multimediale", F.S. "Interventi e servizi per gli studenti- Convitto e Semiconvitto", F.S. "Interventi e servizi per gli studenti".
- Realizzazione di una riunione dei Coordinatori di Dipartimento per discutere delle attività relative all'E-policy.

Azioni da svolgere nei prossimi 3 anni:

- Realizzazione di un sistema di monitoraggio delle attività di prevenzione e formazione (somministrazione a campione nelle classi prime sulle azioni di prevenzione del bullismo e del cyberbullismo);
- Monitoraggio dell'efficacia dell'E-policy attraverso sondaggio rivolto a tutte le componenti dell'Istituto;
- Formazione del personale docente e non docente sui reati on-line e sulla privacy;
- Revisione del Regolamento d'Istituto;
- Implementazione della dotazione tecnica delle classi, per quanto concerne LIM, PC, tablet (anche in comodato d'uso agli studenti) con particolare attenzione nei confronti degli allievi con BES, nei limiti delle dotazioni finanziarie dell'Istituto e dei fondi dedicati.

# 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.

**Area 1: alfabetizzazione e dati**

L'uso del computer è un requisito ormai essenziale per gli studi e per la maggior parte delle professioni, senza queste competenze le persone rimarrebbero escluse dai processi di selezione aziendali.

Alfabetizzazione informatica

Per il raggiungimento dell'obiettivo di alfabetizzazione si intende favorire l'apprendimento delle tecnologie informatiche sviluppando i seguenti contenuti.

Classi: Primo biennio di tutti gli indirizzi

Figure coinvolte

docenti interni alla scuola;

professionisti esterni alla scuola e esperti nel digitale.

Metodologie

Cooperative learning, project work

Contenuti da sviluppare

Parte prima

Hardware e software, Il sistema operativo: ruolo e funzionalità, L'interfaccia dei programmi, Risorse del computer e loro gestione, Organizzazione dei files e dei dati sul disco.

Preservare la sicurezza di un personal computer: l'antivirus per contrastare programmi dannosi per il computer e il backup per creare una copia di sicurezza dei propri dati.

Elaborazione Testi e formattazione di un documento

Parte seconda

Fogli elettronici e impostazioni delle formule aritmetiche

Parte terza

Come si accede a Internet: i provider, il modem router, le connessioni via cavo e WiFi.

La navigazione su Internet: che cos'è il World Wide Web, che cos'è un sito web e come si accede, uso del browser (che cos'è un URL, i preferiti, le schede, le opzioni, la cronologia, i cookies, i plug-in), trovare le informazioni con i motori di ricerca (Google).

Google oltre il motore di ricerca di documenti: immagini, mappe, news, traduzioni.

Comunicazione con la posta elettronica: funzionamento, creare la propria casella di posta, inviare email, ricevere email, gestire le email in cartelle, la sicurezza (spam e il phishing).

Comunicazione in tempo reale e social network

Condivisione multimediale

Alfabetizzazione digitale

L'alfabetizzazione digitale, come definita da Paul Gilster, è la capacità di comprendere e utilizzare le informazioni in diversi formati, a partire da una vasta gamma di fonti accessibili tramite computer. È la capacità di trovare, valutare, utilizzare, condividere e creare contenuti utilizzando le tecnologie dell'informazione e Internet (Cornell

University nel 2009) richiedendo sia abilità cognitive che tecniche (American Library Association nel 2013)

La carenza nelle competenze digitali genera  un problema di inclusione sociale perché chi non è alfabetizzato non può utilizzare i servizi dell'amministrazione pubblica e quelli sanitarie.

Classi: quinquennio

Figure coinvolte:

docenti, interni alla scuola, anche nell'ambito dell'insegnamento dell'educazione civica (area della cittadinanza digitale) nel curricolo;

professionisti esterni alla scuola e esperti nel digitale

Metodologie

Cooperative learning, project work, MLTV

Obiettivi da conseguire:

1. avere una certa familiarità con i luoghi online in cui è possibile trovare informazioni;

2. essere in grado di utilizzare le giuste keyword per portare avanti la propria ricerca (indicizzazione online)

3. avvalersi di strumenti che si occupano della raccolta di materiali provenienti da fonti diverse;

4. essere capace di valutare la validità di una fonte, facendo particolare attenzione al fenomeno noto come "fake news".

5. valutare e gestire dati, informazioni e contenuti digitali;

6. 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: la comunicazione e la collaborazione**

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

Classi: biennio

Figure coinvolte:

docenti, interni alla scuola, anche nell'ambito dell'insegnamento dell'educazione civica (area della cittadinanza digitale) nel curricolo;

referente bullismo e cyberbullismo;

USR, Osservatorio regionale sul bullismo;

amministrazione comunale, servizi socio-educativi;

professionisti esterni alla scuola e esperti nel digitale

Metodologie

Cooperative learning, project work, MLTV, didattica laboratoriale

L'obiettivo generale è quello di consentire al cittadino di essere in grado di interagire con gli altri attraverso le tecnologie, condividendo informazioni attraverso le stesse, potendo quindi partecipare alla vita sociale ed usufruendo i benefici della cosiddetta "cittadinanza digitale". A tal proposito, deve conoscere le regole minime della rete e deve saper creare e gestire un'identità digitale.

INTERAGIRE CON GLI ALTRI ATTRAVERSO LE TECNOLOGIE

A livello minimo e con l'aiuto di qualcuno l'utente dovrà essere in grado di scegliere tecnologie digitali semplici per l'interazione e individuare semplici mezzi di comunicazione adeguati ad un determinato contesto.

Esempio: l'utente è in grado di utilizzare una chat di uso comune sul proprio smartphone (ad es. facebook, messenger o WhatsApp) per parlare con amici e colleghi e organizzare attività di gruppo.

CONDIVIDERE INFORMAZIONI ATTRAVERSO LE TECNOLOGIE DIGITALI

Essere in grado di riconoscere semplici tecnologie digitali appropriate per condividere dati, informazioni e contenuti digitali

ESERCITARE LA CITTADINANZA ATTRAVERSO LE TECNOLOGIE DIGITALI

Essere in grado di individuare semplici servizi digitali per partecipare alla vita sociale, riconoscere semplici tecnologie digitali appropriate per potenziare le proprie capacità personali e professionali e partecipare come cittadino alla vita sociale, per esempio effettuare un sondaggio.

COLLABORARE ATTRAVERSO LE TECNOLOGIE DIGITALI

Essere in grado di scegliere strumenti e tecnologie digitali semplici per i processi

collaborativi, per esempio deve essere in grado di utilizzare gli strumenti digitali più appropriati al lavoro (ad es. Dropbox, Onedrive, Google Drive) per creare con i propri colleghi o amici del materiale di comunicazione.

COMPETENZE DIGITALI DI BASE PER I CITTADINI E NETIQUETTE

Essere in grado di conoscere le norme comportamentali e il know-how per l'utilizzo delle tecnologie digitali e l'interazione con gli ambienti digitali, scegliere semplici modalità di comunicazione e strategie adatte mantenendo toni e linguaggi rispettosi della netiquette.

GESTIRE L'IDENTITÀ DIGITALE

Essere in grado di individuare un'identità digitale, descrivere semplicemente come proteggere la propria reputazione online, riconoscere dati semplici, prodotti attraverso strumenti, ambienti o servizi digitali, di identificare le modalità di creazione di una identità digitale (es: SPID).

**Area 3: La creazione di contenuti digitali (inclusa la programmazione)**

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.).

Classi: quinquennio

Figure coinvolte:

docenti, interni alla scuola, anche nell'ambito dell'insegnamento dell'educazione civica (area della cittadinanza digitale) nel curricolo;

professionisti esterni alla scuola e esperti nel digitale

Metodologie

Cooperative learning, project work, didattica laboratoriale

Obiettivi da conseguire in termini di competenze:

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

2. conoscere un linguaggio di programmazione;

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

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

Area 4: La sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza),

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.

Classi: biennio

Figure coinvolte:

docenti, interni alla scuola, anche nell'ambito dell'insegnamento dell'educazione civica (area della cittadinanza digitale) nel curricolo;

referente bullismo e cyberbullismo;

USR, Osservatorio regionale sul bullismo, Polizia di Stato;

amministrazione comunale, servizi socio-educativi.

Metodologie

Cooperative learning, project work, MLTV, didattica laboratoriale

Obiettivi da conseguire:

1. imparare a proteggere i dispositivi e i contenuti digitali e comprendere i rischi e le minacce presenti negli ambienti digitali. Conoscere le misure di sicurezza e protezione e tenere in debita considerazione l'affidabilità e la privacy;

2. proteggere i dati personali e la privacy negli ambienti digitali. Capire come utilizzare e condividere informazioni personali proteggendo se stessi e gli altri dai danni. Comprendere che i servizi digitali hanno un "regolamento sulla privacy" per informare gli utenti sull'utilizzo dei dati personali raccolti;

3. conoscere (ed esercitare) i propri diritti in termini di privacy e sicurezza.

**Area 5: la risoluzione di problemi e il pensiero critico**

Classi: quinquennio

Figure coinvolte:

docenti, interni alla scuola;

professionisti esterni alla scuola e esperti nel digitale

Metodologia

Cooperative learning, project work, MLTV, didattica laboratoriale

Obiettivi da conseguire:

RISOLVERE PROBLEMI TECNICI

Essere in grado di individuare semplici problemi tecnici nell'utilizzo dei dispositivi e delle tecnologie digitali e identificare semplici soluzioni per risolverli.

INDIVIDUARE BISOGNI E RISPOSTE TECNOLOGICHE

Essere in grado di individuare esigenze, riconoscere semplici strumenti digitali e possibili risposte tecnologiche per soddisfarli, scegliere semplici modalità per adattare e personalizzare gli ambienti digitali alle esigenze personali.

UTILIZZARE IN MODO CREATIVO LE TECNOLOGIE DIGITALI

Mostrare interesse a livello individuale e collettivo nei processi cognitivi semplici per comprendere e risolvere problemi concettuali e situazioni problematiche negli ambienti digitali, come per esempio individuare una piattaforma per richiedere informazioni ben definite su un argomento.

INDIVIDUARE I DIVARI DI COMPETENZE DIGITALI Essere in grado di riconoscere gli aspetti da migliorare o aggiornare le proprie competenze digitali e individuare opportunità di crescita personale e tenersi al passo con l'evoluzione digitale.

---

# *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'IIS "Pischedda" ha una buona dotazione informatica con LIM in tutte le aule, moderni laboratori di informatica, kit di tablet e calcolatrici grafiche ad uso degli studenti in classe e di computer portatili forniti in comodato d'uso, rete con fibra a 200 MB per la didattica e wifi capillare in tutte le aree dell'Istituto. Oltre al sito web https://www.iisgapischeddabosa.edu.it/, l'Istituto possiede il dominio dedicato

@iispischeddabosa.net, sulla piattaforma G-Suite, con account per tutti i docenti e per tutti gli studenti e le studentesse.

L'Istituto riconosce e favorisce la partecipazione del personale ad iniziative di formazione e aggiornamento promosse direttamente dalla scuola, dalle reti di scuole cui esso appartiene, quali Avanguardie Educative della quale l'IIS "Pischedda" è scuola polo, e quelle liberamente scelte dai docenti, in coerenza con il Piano triennale per la formazione e con il Piano d'intervento dell'animatrice digitale.

Gli insegnanti grazie alla possibilità di formazione permanente sono in grado di aggiornare le proprie competenze digitali per l'innovazione didattica e metodologica e di rispondere ai diversi bisogni formativi degli studenti e delle studentesse in modo da accompagnarli ad "imparare a nuotare nell'oceano digitale", secondo l'espressione utilizzata dal quadro di riferimento per le competenze digitali dei cittadini.

---

## *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.

All'interno delle iniziative di formazione e di aggiornamento programmate nel Piano triennale dell'offerta formativa e attuate dal nostro Istituto sono previsti specifici momenti di formazione permanente per gli insegnanti, che mettono al centro l'uso corretto delle tecnologie digitali e delle potenzialità della Rete.

Nel triennio 2021/2024 l'IIS Pischedda attuerà azioni specifiche, secondo il seguente cronoprogramma:

-Analisi del fabbisogno formativo degli insegnanti sull'utilizzo consapevole e sicuro della Rete e sui rischi di quest'ultima;

-Promozione della partecipazione dei docenti a corsi di formazione su tali argomenti;

-Monitoraggio delle azioni svolte attraverso momenti di valutazione;

-Organizzazione di incontri con professionisti della scuola o con esperti esterni.

La formazione dei docenti non sarà finalizzata esclusivamente all'alfabetizzazione ai media ma anche all'attenta valutazione della sfera emotiva e affettiva degli studenti e delle studentesse, che usano le nuove tecnologie per comunicare, esprimere se stessi e sviluppare l'identità personale e sociale.

Nel contempo verrà predisposta un'area specifica sul sito dell'Istituto per la condivisione di materiali informativi, nell'ottica di creare un'ulteriore sinergia fra scuola, studenti/studentesse e famiglie, di promuovere la condivisione di buone pratiche nell'utilizzo consapevole delle TIC e di prevenire e contrastare ogni forma di discriminazione, offesa, denigrazione e lesione della dignità dell'altro, nonché fenomeni di bullismo e cyberbullismo.

Sul sito dell'Istituto è possibile prendere visione del Piano di prevenzione bullismo e cyberbullismo.

Sul sito del progetto "Generazioni connesse", sono diponibili ulteriori approfondimenti, aggiornamenti e strumenti didattici per i docenti.

---

# *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.

La Mission dell'IIS "Pischedda" è quella di "formare persone in grado di pensare ed agire autonomamente e responsabilmente all'interno della società, strutturando un progetto globale che, attraverso lo strumento giuridico dell'autonomia, coinvolga tutti i soggetti protagonisti del processo di crescita: lo studente, la famiglia, i docenti ed il

Territorio."

La famiglia condivide con la Scuola il "Patto di Corresponsabilità" finalizzato a "rafforzare il rapporto scuola/famiglia in quanto nasce da una comune assunzione di responsabilità e impegna entrambe le componenti a condividerne i contenuti e a rispettarne gli impegni", come auspicano le Linee di indirizzo pubblicate dal MIUR.

La Scuola, nell'ottica di un costante coinvolgimento delle famiglie nell'educazione digitale dei propri figli, oltre a predisporre un'area specifica sul sito dell'Istituto per la condivisione di materiali informativi, fornisce consigli e linee guida sull'uso delle tecnologie digitali e segnala la sezione dedicata ai genitori del sito del progetto "Generazioni connesse" dove sono disponibili ulteriori approfondimenti.

Sul sito dell'Istituto è possibile prendere visione del Regolamento d'Istituto

## *Il nostro piano d'azioni*

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

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

- 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 consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.

# 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 è impegnata in prima persona nella tutela della privacy degli utenti attraverso l'applicazione del regolamento d'Istituto e del patto di corresponsabilità.

Particolare attenzione è data dalla nostra Istituzione, nei confronti degli studenti quando questi sono minorenni, in ottemperanza all'articolo 8 della Carta dei diritti fondamentali dell'Unione europea tutelato dal regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, recepito dal nostro ordinamento dal D.Lgs. 10 agosto 2018 n. 101, entrato in vigore il 19 settembre 2018.

In particolare, la nostra scuola ha attivato una specifica sezione Privacy sul sito web dell'istituto dove sono state pubblicate tutte le informative e i relativi moduli per l'acquisizione dei consensi, i vari DPIA (Data Protection Impact Assessment), la politica sulla protezione dei dati personali, vari regolamenti, diverse informative sulla Privacy, organigramma.

---

# *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.

In particolare, da quando è iniziata l’emergenza sanitaria ancora in atto è emersa prepotentemente la necessità dell’uso delle TIC per lo svolgimento della didattica in DAD e in DDI, modalità che hanno permesso lo svolgimento delle attività didattiche a distanza.

Il nostro Istituto gode di una strumentazione tecnologica abbastanza ricca e varia, LIM in ogni aula, notebook disponibili sia per la didattica in classe che per il comodato d’uso agli studenti che ne avessero la necessità, tablet per particolari attività di classe ecc. La strumentazione è diffusa capillarmente in tutti gli spazi ed è stata acquistata grazie ai finanziamenti europei statali PON, a quelli della Regione Sardegna (progetto Semid@s), ai progetti del Piano Nazionale Scuola Digitale e alla Fondazione di Sardegna.

La connettività 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 nostra scuola, costituita da due plessi e da un convitto, ha tre linee in fibra ottica (una per ciascuna sede) e una linea in fibra ottica riservata alla segreteria.

I due plessi sono quasi per intero cablati, con la possibilità di collegarsi ad internet via cavo da quasi tutte le aule e laboratori didattici. Inoltre è presente una rete Wi-Fi che copre per intero tutti i locali delle varie sedi con l’utilizzo di vari access point.

L’accesso alla rete Wi-Fi è protetto da password adeguate, ed è controllato e monitorato dai tecnici informatici del nostro Istituto. E’ vietato l'uso dei dispositivi personali se non espressamente autorizzati dai docenti per fini esclusivamente didattici.

La rete della segreteria è separata dalla rete didattica e, grazie ad un server dedicato, gestisce in modo autonomo e con regole differenti la sicurezza. Per la gestione della privacy e della sicurezza informatica della segreteria e del registro elettronico la nostra scuola si appoggia alla ditta specializzata Vargiu di Cagliari.

---

# 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.

Fra gli strumenti di comunicazione esterna, il nostro Istituto usa soprattutto il sito web della scuola.

Come strumenti di comunicazione interna usa il registro elettronico, un sistema di e-mail (una normale e una pec per la segreteria, una riservata per alunni e docenti), applicativi e piattaforme di lavoro collaborativo e condiviso.

Il registro elettronico permette di gestire la comunicazione con le famiglie, le quali attraverso di esso possono visualizzare molte informazioni utili, interagendo con la scuola, su:

andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari);

risultati scolastici (voti, documenti di valutazione); udienze (prenotazioni colloqui individuali);

eventi (agenda eventi);

comunicazione varie (comunicazioni di classe, comunicazioni personali, ecc).

Grazie all'uso delle tecnologie digitali si è potuti passare ad una comunicazione multimediale, bidirezionale e interattiva.

Dal mese di marzo dell'anno scolastico 2019\2020, periodo di inizio dell'emergenza sanitaria ancora in atto che ha portato la scuola a modalità di didattica a distanza, la nostra scuola ha utilizzato il pacchetto applicativo GSuite di Google, sia per lezioni che per le riunioni e gli incontri con i genitori.

Ciò naturalmente ha rappresentato un'opportunità significativa anche in termini di un maggiore coinvolgimento degli studenti o dei genitori, con la possibilità di usare diversi linguaggi (scrittura, immagini, video etc.) ma in taluni casi può anche rivelarsi un problema non sempre facile da gestire.

Pertanto abbiamo elaborato un regolamento relativo alla Didattica a Distanza e alla Didattica Digitale Integrata.

---

# *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.

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 allievi 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( se autorizzata) viene fatta su rete personale.

§ Per le comunicazioni di necessità tra famiglia e studente, saranno utilizzate le

strutture della scuola.

**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 estremamente urgente.

Resta la responsabilità deontologica e professionale del dirigente, dei docenti e del personale ATA che hanno il dovere di vigilare sui comportamenti degli studenti e delle studentesse il quale sussiste in tutti gli spazi scolastici e di segnalare eventuali infrazioni suscettibili di sanzioni disciplinari.

## *Il nostro piano d'azioni*

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

La nostra scuola ha già organizzato e partecipato ad eventi riguardanti la sicurezza informatica per gli alunni\e, per i Docenti e per il personale ATA. Comunque nei prossimi anni scolastici intende ancora:

§ Organizzare uno o più eventi o attività volti a formare gli studenti, le studentesse, i Docenti e il personale ATA 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).

# 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 comportamenti a rischio possono essere molteplici ma afferiscono, in base alla fascia di età, a uno sviluppo cognitivo, affettivo e morale incompleto oppure a fasi critiche transitorie o alla capacità di gestione di dinamiche complesse, mediante confronto/relazione con il Sé e l'altro, mediante la dimensione dell'empatia, della socialità, dell'affettività e della sessualità, e mediante il riconoscimento di un limite tra

dimensione di legalità ed utilizzo sicuro delle tecnologie digitali.

La necessità di sensibilizzare gli studenti ad un utilizzo sicuro e consapevole delle tecnologie digitali, sia in un'ottica di tutela dai rischi potenziali che di valorizzazione delle opportunità esistenti, pone tutta la comunità educante di fronte alla sfida di riconsiderare la propria identità, le proprie risorse e il proprio ruolo educativo. L'Istituto intende perseguire azioni di prevenzione universale e di sensibilizzazione, attraverso un'efficace integrazione con la rete dei servizi territoriali locali (Polizia postale, Polizia di Stato, ASL...), al fine di formare e consolidare quelle competenze educative di base necessarie a poter gestire le situazioni di vita che i ragazzi sperimentano online.

---

# *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).

Un'indicazione operativa da tener presente per intervenire efficacemente è anche capire se si tratta effettivamente di cyberbullismo o di altra tipologia di comportamenti violenti o disfunzionali. Oltre al contesto, altri elementi utili ad effettuare questa valutazione sono le modalità in cui avvengono (alla presenza di un "pubblico"? Tra coetanei? In modo cronico e intenzionale? etc.) e l'età dei protagonisti. 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.

La necessità di sensibilizzare gli studenti ad un utilizzo sicuro e consapevole delle tecnologie digitali, sia in un'ottica di tutela dai rischi potenziali che di valorizzazione delle opportunità esistenti, pone tutta la comunità educante di fronte alla sfida di riconsiderare la propria identità, le proprie risorse e il proprio ruolo educativo.

Finalità condivisa tra scuola e famiglia è intervenire preventivamente ed efficacemente, al fine di evitare, arginare ed eliminare possibili manifestazioni di comportamenti antisociali.

L'Istituto intende perseguire azioni di prevenzione e di sensibilizzazione:

· accrescere le capacità di intervento, sia in ottica preventiva, sia di gestione degli episodi già verificatisi;

· promuovere negli studenti buone prassi comportamentali;

· supportare docenti e famiglie in momenti di difficoltà;

· promuovere la sicurezza in Rete degli studenti, perché acquisiscano le competenze necessarie all'esercizio di una cittadinanza digitale consapevole;

· valutare i comportamenti che sfociano in disagio sociale, con la possibilità di coinvolgere anche un servizio specialistico socio-sanitario (Psicologo della scuolaServizi di Neuropsichiatria, etc.), quale supporto e/o forme di mediazione;

· attivare un'efficace integrazione con la rete dei servizi territoriali locali (Polizia postale, Questura, ASL etc...), 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). A tal fine di formare e consolidare quelle competenze educative di base necessarie a poter gestire le situazioni di vita che i ragazzi sperimentano online.

---

# *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.

· Sviluppo delle competenze digitali ed educazione ad un uso etico e consapevole delle tecnologie e dei social network;

· Valorizzare la dimensione relazionale dei più giovani, sensibilizzandoli verso capacità di analisi e discernimento, per fornire 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;

· partecipazione ad eventi e incontri con consulenti/esperti esterni (Carabinieri, Polizia Postale, Polizia di Stato, associazioni del Territorio…), per la prevenzione e la sensibilizzazione sui reati legati all'utilizzo di internet e delle piattaforme on-line;

· presenza a scuola di referente bullismo e cyberbullismo e/o di referente dello

Sportello d'ascolto.

---

# 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?*

Tale dipendenza, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica, che deve fornire gli strumenti agli studenti e alle studentesse la consapevolezza dei rischi che comporta l'"iper-connessione".

Pertanto l'Istituto si propone di promuovere azioni di prevenzione attraverso percorsi sul "benessere digitale", ossia la capacità di creare e mantenere una relazione sana con la tecnologia

Gli elementi che contribuiscono al benessere digitale sono:

· la ricerca di equilibrio nelle relazioni anche online, l'uso degli strumenti digitali per il raggiungimento di obiettivi personali;

· la capacità di interagire negli ambienti digitali in modo sicuro e responsabile;

· la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche).

Se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi. È importante non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli studenti e delle studentesse, strutturando chiare e semplici regole condivise. Inoltre, sarà fondamentale concordare una linea condivisa con la famiglia, per stabilire mezzi e modalità durante lo studio domestico, con forme di controllo attivo durante la navigazione in Rete.

---

# 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.

Spesso tali immagini o video, anche se inviate ad una stretta cerchia di persone, si diffondono in modo incontrollabile, perchè facilmente modificabili, scaricabili e condivisibili, e possono creare seri problemi, sia personali che legali, alla persona ritratta. L’invio di foto che riguardano minorenni in pose sessualmente esplicite configura, infatti, 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. I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell’altro/i e depressione.

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

· Sviluppo delle competenze digitali ed educazione ad un uso etico e consapevole delle tecnologie e dei social network;

· Valorizzare la dimensione relazionale dei più giovani, sensibilizzandoli verso capacità di analisi e discernimento, per fornire 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;

· Partecipazione ad eventi e incontri con consulenti/esperti esterni (Carabinieri, Polizia Postale, Polizia di Stato, associazioni del Territorio…), per la prevenzione e la sensibilizzazione sui reati legati all'utilizzo di internet e delle piattaforme on-line;

· Presenza a scuola di referente bullismo e cyberbullismo e/o di referente dello Sportello d'ascolto.

---

# 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.

Per riconoscere un eventuale caso di adescamento online è importante prestare attenzione a piccoli segnali che possono essere indicatori importanti, per valutare un cambiamento improvviso nel comportamento di un minore:

· Il minore ha conoscenze sessuali non adeguate alla sua età?

· Venite a conoscenza di un certo video o di una foto che circola online o -ancora- il minore ha ricevuto un contenuto (o filmato), ma c'è imbarazzo e preoccupazione nel raccontarvi di più… Il minore si isola totalmente e sembra preso solo da una relazione online?

· Ci sono prese in giro e allusioni sessuali verso un bambino/ragazzo in particolare?

Al fine di prevenire casi di adescamento online è opportuno accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. È 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. Fondamentale quindi, è portare avanti un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da

come realmente è). Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere, ad esempio, all'adescatore. È importante che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove.

Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo 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.

---

# *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.**

Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia. L'intento è quello di facilitare il processo di rimozione del materiale stesso dalla Rete e allo stesso tempo consentire le opportune attività investigative finalizzate ad identificare chi possiede quel materiale, chi lo diffonde e chi lo produce, ma, soprattutto e primariamente, ad identificare i minori abusati presenti nelle immagini e video, assicurando la fine di un abuso che potrebbe essere ancora in corso e il supporto necessario. Parallelamente, per salvaguardare il benessere psicofisico degli alunni coinvolti nella visione di questi contenuti, 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, etc.) Se si è a conoscenza di tale tipologia di reato è possibile far riferimento alla Polizia di Stato, Compartimento di Polizia postale e delle Comunicazioni, Arma dei Carabinieri.

Studi in materia dimostrano come l'utilizzo di materiale pedopornografico possa essere propedeutico all'abuso sessuale agito ed è quindi fondamentale, in termini preventivi, intervenire per ridurre l'incidenza di tale possibilità. L'abuso sessuale online rappresenta una particolare declinazione dell'abuso sessuale su bambini/e, ragazzi/e, la cui caratteristica fondante è il ruolo ricoperto dalle tecnologie digitali, le quali diventano il mezzo principale attraverso cui l'abuso viene perpetrato, documentato e diffuso in Rete con immagini e/o video. Le dinamiche attraverso cui l'abuso sessuale

online si manifesta producono effetti sulle vittime che si aggiungono e moltiplicano a quelli associati all'abuso sessuale.

## Il nostro piano d'azioni

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

□ 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.

□ Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.

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

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

□ Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

□ Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.

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

# 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.

**Trattamento dei casi**

Per poter rilevare i casi acuti o di emergenza è importante che la scuola attivi 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.

In relazione alle segnalazioni, è importante porre in essere una prima valutazione di gravità e una solerte decisione sulle azioni da intraprendere.

Quando si verificano episodi acuti di bullismo, la prima azione deve essere orientata alla tutela della vittima, includendo, successivamente, il bullo/prevaricatore e il gruppo classe.

In generale, in caso di episodio sospetto e/o denunciato, si suggerisce di seguire il seguente schema di intervento:

- colloquio individuale con la vittima;
- colloquio individuale con il bullo;
- possibile colloquio con i bulli insieme (in caso di gruppo);
- possibile colloquio con vittima e bullo/i se le condizioni di consapevolezza lo consentono;
- coinvolgimento dei genitori di vittima e bullo/i.

Tuttavia, essendo ogni situazione di bullismo differente in termini di modalità, è opportuno valutare di volta in volta quale sia l'ordine più efficace. Si ricorda che, in base alle norme vigenti:

- in caso di rilevanza penale del comportamento è obbligo della scuola segnalare

l'evento all'autorità giudiziaria;

■ in caso di segnalazione di episodi di cyberbullismo, il Dirigente scolastico ha l'obbligo

di informare tempestivamente la famiglia come indicato nella L.71/2017.

Si consiglia, in ogni caso, una preventiva consultazione con il Team Antibullismo e il Team per l'Emergenza al fine di concordare al meglio le comunicazioni ed eventuali strategie di intervento.

**L'INTERVENTO IN CASI ACCERTATI**

La maniera migliore per prevenire e contrastare il fenomeno del bullismo e del cyberbullismo è quella di adottare una politica scolastica integrata consistente in un insieme coordinato di azioni in cui siano coinvolte tutte le componenti scolastiche ed in cui tutti gli adulti (Dirigente, docenti, personale non docente, genitori) si assumano la responsabilità di entrare in relazione con gli alunni e di fornire prima di tutto informazioni ed aiuto. Il recupero dei "bulli" e dei "cyber-bulli" può avvenire solo attraverso l'intervento educativo sinergico delle agenzie preposte alla loro educazione e quindi, famiglia, scuola, istituzioni. A fianco dell'intervento educativo-preventivo, si dovranno tuttavia applicare nei confronti dei bulli e dei cyber-bulli delle misure disciplinari e delle misure di intervento che dimostrino chiaramente che la scuola

CONDANNA FERMAMENTE

i soprusi, i comportamenti aggressivi ed ogni forma di prepotenza, sia online sia offline!!

Procedura scolastica da attivare in caso di atti di bullismo e cyberbullismo

1. Il docente che viene a conoscenza di un atto configurabile come bullismo o cyberbullismo deve:

- Informare subito il Dirigente Scolastico (o in sua assenza i collaboratori del DS o il fiduciario di plesso) e il referente di Istituto per la prevenzione del bullismo e cyberbullismo;

- Informare il Coordinatore di classe, che provvederà ad avvisare i colleghi del Consiglio.

2. Il Dirigente, o un docente da lui delegato, raccoglierà informazioni sull'accaduto, attraverso interviste e colloqui; verranno raccolte le diverse versioni e ricostruiti i fatti ed i punti di vista, raccolto eventualmente materiale (chat di social, video, messaggi, testimonianze dirette, ecc) attenendosi ai soli fatti accaduti e riportandoli per iscritto in ordine cronologico. È necessario creare un clima di empatia, di solidarietà e di disponibilità al confronto che permetta un'oggettiva raccolta di informazioni.

3. Il Dirigente, o un docente da lui delegato, informa il/i docente referente, individuato presso ciascuna istituzione scolastica "con il compito di coordinare le

iniziative di prevenzione e di contrasto del cyberbullismo, anche avvalendosi della collaborazione delle Forze di polizia nonché delle associazioni e dei centri di aggregazione giovanile presenti sul territorio" (art.4.3, L.72/2017)

4. Il Dirigente fa convocare separatamente le famiglie degli alunni coinvolti a vario titolo, prima telefonicamente e poi con comunicazione scritta formale.

5. Incontrando i genitori degli alunni coinvolti, il Dirigente, o un docente da lui delegato, espone i fatti accaduti, richiamando la responsabilità educativa che grava sulla famiglia nel comportamento del figlio a scuola in presenza di comportamenti scorretti o violenti. Propone alle famiglie azioni di supporto alla vittima e di intervento sul bullo e ad altri alunni coinvolti in varia misura.

6. Il Dirigente Scolastico convoca il Consiglio di classe, coadiuvato dal docente referente, per analizzare i fatti e prendere le relative decisioni in termini sia disciplinari/sanzionatori che educativi e formativi, mobilitando, se necessario, le risorse disponibili a Scuola (sportello psicopedagogico, esperto cyber bullismo…) e sul territorio (Servizi Sociali, tutela minori, Polizia postale…) e predisponendo una serie di azioni volte a:

• Tutelare la vittima;

• Irrogare le adeguate misure disciplinari, proporzionate all'offesa, quali:

lettera di scuse alla vittima;

compiti/attività a favore della comunità scolastica;

sospensione del diritto a partecipare ad attività complementari ed extrascolastiche;

sospensione da scuola.

• Strutturare, con il coordinamento del docente referente e il coinvolgimento di tutti i docenti del consiglio di classe, una strategia di intervento che permetta il superamento della problematica segnalata attraverso:

responsabilizzazione degli alunni coinvolti;

discussione strutturata in classe;

informazione e coinvolgimento dei genitori;

interventi della psicologa di sportello;

ripristino delle regole di comportamento di classe.

7. Il Referente prevenzione bullismo/cyberbullismo effettuerà il monitoraggio della situazione a breve e medio termine e la valutazione dell'efficacia delle azioni di intervento stabilite dal consiglio di classe, riferendone gli esiti al Dirigente Scolastico.

8. Nell'eventualità che la famiglia non collabori oppure giustifichi i comportamenti del proprio figlio o mostri atteggiamenti oppositivi o comunque inadeguatezza, verrà valutata dal Dirigente Scolastico la segnalazione ai Servizi Sociali del Comune o alla Tutela dei Minori.

**PROTOCOLLO DI INTERVENTO PER UN PRIMO ESAME NEI CASI ACUTI E DI EMERGENZA**

**Intervento con la vittima**

- accogliere la vittima in un luogo tranquillo e riservato;

- mostrare supporto alla vittima e non colpevolizzarla per ciò che è successo;

- far comprendere che la scuola è motivata ad aiutare e sostenere la vittima;

- informare progressivamente la vittima su ciò che accade di volta in volta;

- concordare appuntamenti successivi (per monitorare la situazione e raccogliere ulteriori dettagli utili).

**Intervento con il bullo**

- importante, prima di incontrarlo, essere al corrente di cosa è accaduto;

- accogliere il presunto bullo in una stanza tranquilla, non accennare prima al motivo del colloquio;

- iniziare il colloquio affermando che si è al corrente dello specifico episodio offensivo o di prevaricazione;

- fornire al ragazzo/a l'opportunità di

esprimersi, favorire la sua versione dei fatti;

- mettere il presunto bullo di fronte alla gravità della situazione;

- non entrare in discussioni;

- cercare insieme possibili soluzioni ai comportamenti prevaricatori;

- ottenere, quanto più possibile, che il presunto bullo dimostri comprensione del problema e bisogno di riparazione;

- in caso di più bulli, i colloqui avvengono preferibilmente in modo individuale con ognuno di loro, uno di seguito all'altro, in modo che non vi sia la possibilità di incontrarsi e parlarsi;

- una volta che tutti i bulli sono stati ascoltati,

si procede al colloquio di gruppo

**Colloquio di gruppo con i bulli**

- iniziare il confronto riportando quello che è emerso dai colloqui individuali;

- l'obiettivo è far cessare le prevaricazioni

individuando soluzioni positive.

Far incontrare prevaricatore e vittima – questa procedura può essere adottata solo se le parti sono pronte e il Team rileva un genuino senso di pentimento e di riparazione nei prepotenti; è importante:

- ripercorrere l'accaduto lasciando la parola al bullo/i

- ascoltare il vissuto della vittima circa la situazione attuale

- condividere le soluzioni positive e predisporre un piano concreto di cambiamento.

**Coinvolgimento del gruppo classe o di possibili spettatori**

Questa azione si consiglia solo quando possiamo rilevare un chiaro segnale di cambiamento nel presunto bullo (o più di uno) e il coinvolgimento del gruppo non implica esposizioni negative della vittima, ma può facilitare la ricostruzione di un clima e di relazioni positive nella classe.

---

# *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.

# *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.

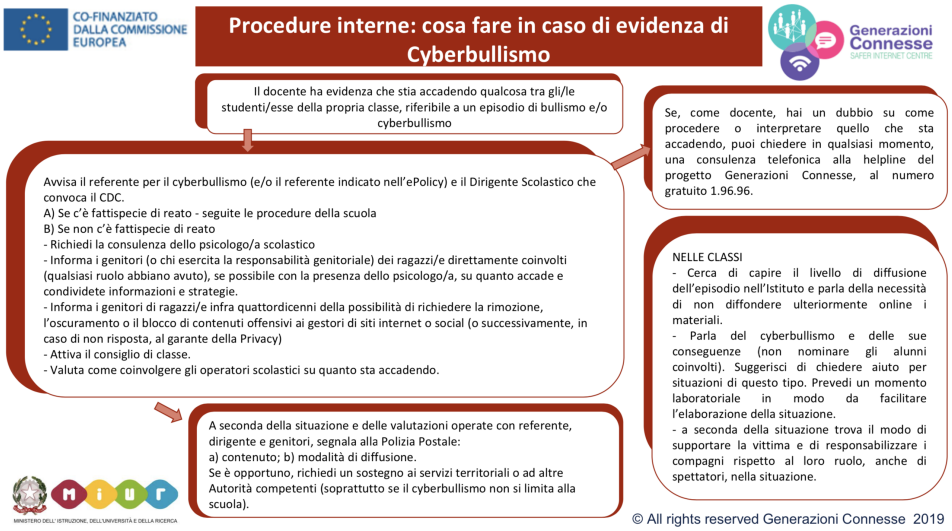
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti

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.

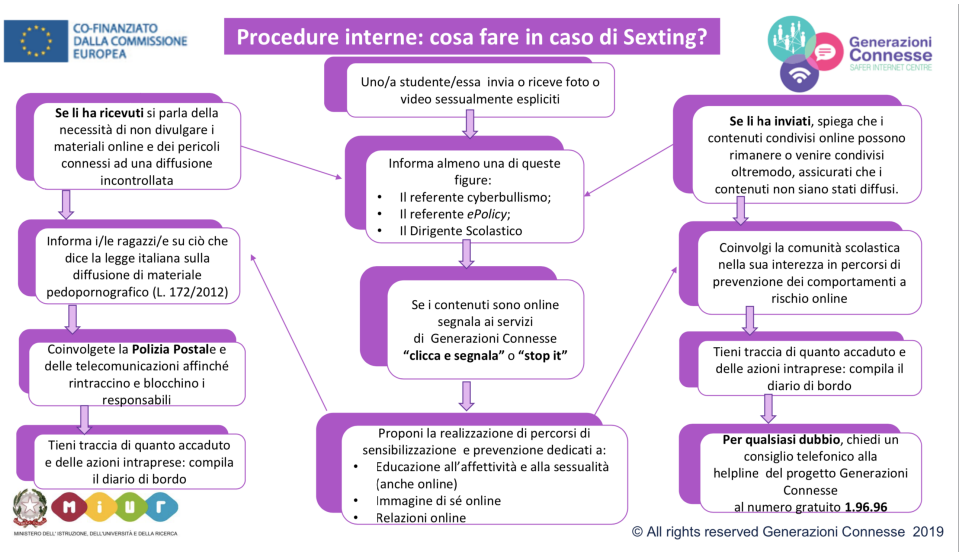
# *5.4. - Allegati con le procedure*

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

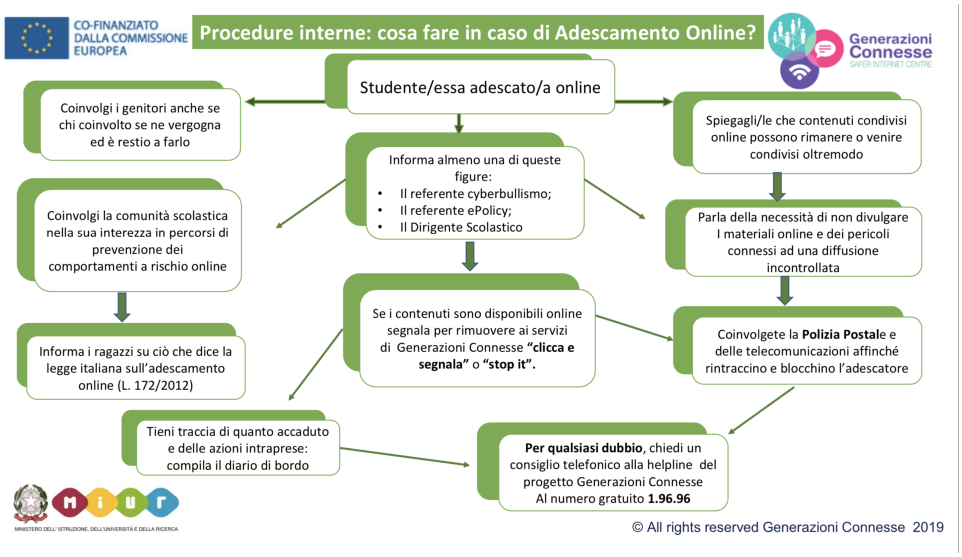




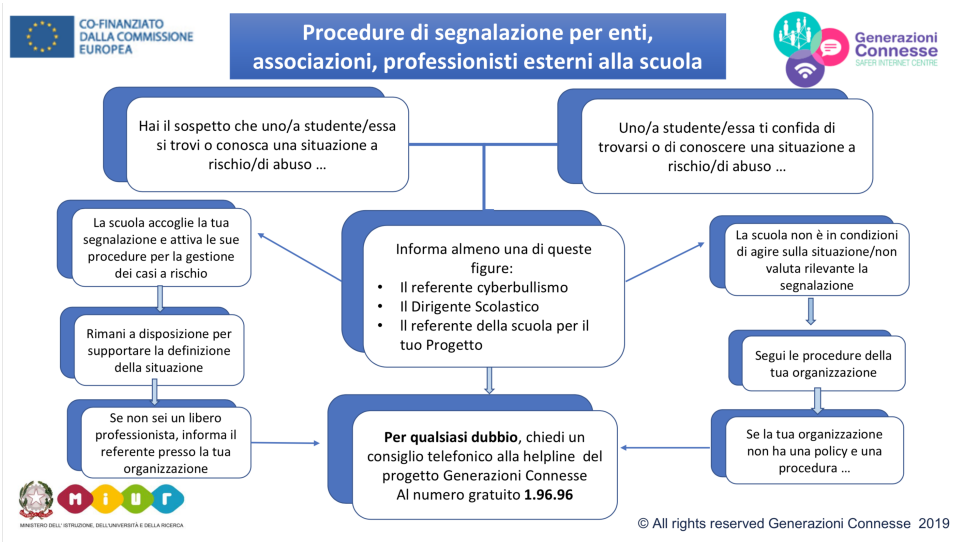
# Procedure interne: cosa fare in caso di sexting?




## 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*

**Non è prevista nessuna azione.**

UDA ROSELLA
30.06.2021
15:07:04 UTC