Documento di ePolicy

BAMM301007

CPIA BAT

VIA COMUNI DI PUGLIA 4 - 76123 - ANDRIA - BARLETTA-ANDRIA-TRANI (BT)

Paolo Farina

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

Perché è importante dotarsi di una E-policy?

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

all’uso di Internet.

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

Il CPIA BAT, Centro Provinciale Istruzione degli Adulti della provincia di Barletta - Andria - Trani, ha elaborato ed adottato il presente documento e-Policy partendo dalle LINEE DI ORIENTAMENTO emanate dal MIUR ad ottobre del 2017 per la prevenzione e il contrasto del cyberbullismo.

Lo scopo della e-Policy è di condividere e stabilire con tutti i membri della comunità scolastica regole, modalità e principi sull’utilizzo consapevole e corretto di internet.

Lo sviluppo delle nuove tecnologie, il loro utilizzo nell’ambito didattico e la maggiore diffusione nella vita di tutti i giorni di questi strumenti richiede maggiore responsabilità e consapevolezza. È compito dell’intera comunità scolastica garantire che gli studenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato e sicuro. Di qui la necessità di dotare la Scuola di una propria Policy di E-safety, anche al fine di gestire le eventuali infrazioni come integrazione del Regolamento d’Istituto.

Il presente documento è stato realizzato tenendo conto delle indicazioni proposte dal progetto GENERAZIONI CONNESSE (www.generazioniconnesse.it) realizzato su indicazioni del MIUR e della COMMISSIONE EUROPEA col supporto di: Polizia Postale, Garante per l’Infanzia e associazioni che operano in difesa dei diritti dei ragazzi; riteniamo che, anche se il CPIA si rivolge in particolare all'Istruzione degli Adulti, l'ePolicy potrà essere un punto di partenza per la diffusione e condivisione di buone pratiche della sicurezza in rete, a cominciare dall'utilizzo consapevole dei propri dispositivi digitali.

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 nostra scuola, nel farsi carico della formazione globale sia di individui nella fase evolutiva che di persone adulte, deve individuare in maniera chiara e inequivocabile

ruoli e responsabilità di ciascuno degli attori del percorso formativo.

Nella promozione dell'uso consapevole della rete

- Il **Dirigente Scolastico** deve:

- garantire la corretta formazione del personale scolastico sulle tematiche relative all'uso sicuro e consapevole di Internet e della rete;
- garantire una formazione adeguata del personale docente relativo all'uso delle TIC nella didattica;
- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di Internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;
- seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.

- L'**Animatore digitale**, supportato dal Team dell'innovazione, deve:

- stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale"e fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite password efficaci e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione);
- coinvolgere la comunità scolastica (alunni, famiglie e altri attori del territorio) nella partecipazione ad attività e progetti attinenti alla "scuola digitale".

- Il **referente del bullismo e cyberbullismo** deve:

- coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e cyberbullismo (può avvalersi della collaborazione delle Forze di polizia e Associazioni del territorio).
- coinvolgere (ove possibile), con progetti e percorsi formativi ad hoc, studenti, colleghi e famiglie.

- Il **personale scolastico** (ATA, segreterie, etc) deve:

- essere consapevole dei problemi di sicurezza on-line connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili;

- comprendere e contribuire a promuovere politiche di e-sicurezza;
- monitorare l'uso di dispositivi tecnologici e attuare politiche scolastiche per quanto riguarda questi dispositivi;
- segnalare qualsiasi abuso o problema, anche sospetto, al Dirigente Scolastico e ai responsabili della sicurezza online;
- usare comportamenti sicuri, responsabili e professionali nell'uso della tecnologia;
- garantire che le comunicazioni digitali con gli studenti dovrebbero essere a livello professionale e solo attraverso i sistemi scolastici, non attraverso meccanismi personali, per esempio mail, telefoni cellulari, ecc.
- aver letto, compreso e sottoscritto la presente policy.

- Il **Direttore dei servizi generali e amministrativi** deve:

- assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o ad annosi attacchi esterni;
- garantire il funzionamento dei diversi canali di comunicazione della scuola (circolari, sito web,ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di Internet.

- I **Docenti** devono:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di Internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di Internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantire che gli alunni comprendano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di Internet;
- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete, ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
- garantire che le comunicazioni digitali dei docenti con alunni e famiglie siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare i corsisti a siti controllati e verificati come adatti per il loro uso e controllare che nelle

ricerche su Internet siano trovati e trattati solo materiali idonei;
- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni minorenni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo all'Animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- segnalare al Dirigente scolastico e ai genitori (in caso di minori) qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di Internet, per l'adozione delle procedure previste dalle norme.

- Gli **Alunni** devono:

- essere responsabili nell'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali, ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;
- comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di Internet ai docenti e, se minori, anche alle famiglie.

- I **Genitori** (in caso di alunni minorenni) devono:

- sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle TIC nella didattica;
- seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti;
- relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i figli non usano responsabilmente le tecnologie digitali o Internet;
- fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di Internet e dello smartphone in generale;
- accettare e condividere quanto scritto nell'ePolicy dell'Istituto.

- Gli **Enti esterni e le Associazioni** devono:

- conformarsi alla politica della scuola riguardo l'uso consapevole delle TIC e della Rete;
- promuovere comportamenti sicuri, la sicurezza on-line e assicurare la

protezione degli studenti durante le attività che si svolgono insieme.

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

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

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

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

Le organizzazioni/associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve o/e lungo periodo, dovranno prendere atto di quanto stilato nell' ePolicy dell'Istituto o eventualmente sottoscrivere un'informativa sintetica del documento in questione, presente nel contratto.

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.

La ePolicy è un documento condiviso da tutte le componenti che operano nella scuola:

- ALUNNI:

- saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione;
- l'istruzione degli alunni riguardo all'uso responsabile e sicuro di Internet precederà l'accesso alla rete;
- l'elenco delle regole per la sicurezza on-line potrà essere pubblicato in tutte le aule o laboratori con accesso a Internet;
- sarà data particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili.

- DOCENTI:

- La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di Internet sarà discussa negli organi collegiali e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web;
- per proteggere tutto il personale e gli alunni, la scuola metterà in atto una linea di condotta di utilizzo accettabile, controllato e limitato alle esigenze didattiche essenziali in riferimento alle tecnologie digitali;
- il personale docente sarà reso consapevole del fatto che il traffico in Internet può essere monitorato e si potrà risalire al singolo utente registrato;
- un'adeguata informazione/formazione on-line del personale docente nell'uso sicuro e responsabile di Internet, sia professionalmente che personalmente,

sarà fornita a tutto il personale, anche attraverso il sito web della scuola;
- il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC sarà supervisionato dal collaboratore tecnico, che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici;
- l'Animatore digitale metterà in evidenza on-line utili strumenti che il personale potrà usare con gli alunni in classe. Questi strumenti varieranno a seconda dell'età e della capacità degli alunni;
- tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

- GENITORI in caso di studenti minorenni:

- L'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di Internet sarà attirata nelle news o in altre aree del sito web della scuola;
- sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di Internet in occasione degli incontri assembleari, collegiali e individuali;
- l'Animatore digitale fornirà ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di Internet anche a casa;
- l'Animatore digitale e i docenti di classe forniranno ai genitori indirizzi sul web relativi a risorse utili per lo studio e a siti idonei ed educativi per gli alunni, sistemi di filtraggio e attività educative per il tempo libero.

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) Disciplina degli alunni

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

- un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;
- l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;
- la condivisione di immagini intime;
- la comunicazione incauta e senza permesso con sconosciuti;

- il collegamento a siti web non indicati dai docenti.

Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo dell'alunno. Sono previsti pertanto da parte dei docenti provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento, quali:

- il richiamo verbale;
- il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);
- il richiamo scritto con annotazione sul registro;
- in caso di minori la convocazione dei genitori da parte degli insegnanti;
- in caso di minori la convocazione dei genitori da parte del Dirigente scolastico.
- in caso di studenti maggiorenni la convocazione dell'alunno da parte del Dirigente Scolastico.

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

2) Disciplina del personale scolastico

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

- un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- un utilizzo delle comunicazioni elettroniche con gli alunni e i genitori (in caso di minori) non compatibile con il ruolo professionale;
- un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- una carente istruzione preventiva degli alunni sull'utilizzazione corretta e responsabile delle tecnologie digitali e di Internet;
- una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.

Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a Internet, la posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone una copia per eventuali successive investigazioni.

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

3) Disciplina dei genitori in caso di alunni minorenni

In considerazione dell'età degli alunni e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico.

Le situazioni familiari meno favorevoli sono:

- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai;
- una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio;
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone;
- un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei;
- un utilizzo del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria indirizzi o contenuti non idonei.

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

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.

Tutti gli attori coinvolti vengono informati della pubblicazione del presente "Regolamento per l'uso delle risorse tecnologiche e di rete" della scuola e possono prenderne visione, prioritariamente sul sito istituzionale della scuola.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il monitoraggio dell'implementazione della ePolicy e del suo eventuale aggiornamento sarà curato dal Dirigente Scolastico con la collaborazione dell'Animatore digitale, del Team per l'innovazione e del referente del bullismo e cyberbullismo. Avrà il fine di rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di Internet. Il monitoraggio on-line sarà rivolto anche ai docenti, al fine di valutare l'impatto della ePolicy e la necessità di eventuali miglioramenti.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti e a tutto il personale scolastico

Azioni da svolgere nei prossimi 3 anni:

- Organizzare 1 evento di presentazione dell'ePolicy e del progetto Generazioni Connesse rivolto agli studenti.

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.

Per progettare ed implementare un curricolo digitale, l'Istituzione scolastica prevede di intervenire su tutte le classi di I livello, I e II periodo didattico e nelle classi di alfabetizzazione ove il livello di conoscenza della lingua italiana (L2) sia almeno di A2 da realizzarsi in prospettiva di continuità e trasversalità con le discipline del curricolo scolastico.

L'intervento nelle classi terrà conto delle dimensioni cui si riferiscono le "competenze digitali":

- dimensione tecnologica: fondamentale far riflettere i nostri corsisti sul potenziale delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana, supportandoli nella comprensione della "grammatica" dello strumento al fine di evitare automatismi;
- dimensione cognitiva: si riferisce alla capacità di cercare, usare e creare in

modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità;

- dimensione etica: farà riferimento alla capacità di gestire in modo sicuro i propri dati personali e quelli altrui, e di usare le tecnologie digitali per scopi eticamente accettabili;

- dimensione sociale: pone più l'accento sulle pratiche sociali e quindi sullo sviluppo di particolari abilità socio-comunicative e partecipative.

Nell'ambito del percorso formativo saranno affrontate alcune delle tematiche centrali per lo sviluppo delle competenze digitali: i diritti della rete, a partire dalla Dichiarazione per i Diritti in Internet redatta dalla Commissione per i diritti e i doveri relativi ad Internet della Camera dei Deputati; l'educazione ai media e alle dinamiche sociali online (social network); la qualità, integrità e circolazione dell'informazione (attendibilità delle fonti, diritti e doveri nella circolazione delle opere creative, privacy e protezione dei dati, information literacy).

Facciamo riferimento al **DigComp** che è diventato un modello per lo sviluppo e la pianificazione strategica di iniziative sulle competenze digitali. Il documento prevede, infatti, aree di competenze quali: area 1 - "Alfabetizzazione e dati"; area 2 - "Comunicazione e collaborazione"; area 3 - "Creazione di contenuti digitali" e area 4 - "Sicurezza". Si cercherà di lavorare soprattutto sulle aree 1 e 2 per le classi di alfabetizzazione, mentre per le restanti classi il nostro intervento si focalizzarà su tutte e quattro le aree.

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.

Per formare tutti i docenti dell'Istituto scolastico sull'uso e l'integrazione delle TIC nella didattica, il Collegio dei docenti favorirà la partecipazione del personale ad

iniziative promosse sia direttamente dalla scuola, dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dai docenti (anche online), in coerenza con il piano di formazione.

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

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

Al fine di promuovere la formazione dei docenti sull'uso responsabile e sicuro della Rete e dei rischi ad essa collegati, si potrebbe pensare ad un cronoprogramma che consideri il triennio scolastico in un'ottica di vera e propria programmazione, con le seguenti azioni specifiche:

- somministrazione di un questionario per personalizzare il fabbisogno formativo degli insegnanti sull'uso sicuro della Rete;
- informazione e promozione della partecipazione dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto "Generazioni Connesse";
- monitoraggio in itinere delle azioni svolte , attraverso un sondaggio online;
- massima visibilità ad incontri con professionisti della scuola e/o con esperti esterni, enti/associazioni, etc., che di volta in volta si rendessero necessari;
- diffusione di materiale informativo sul sito della scuola.

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.

Per rinforzare la partnership educativa fra scuola, famiglie dei minori iscritti e adulti frequentanti, il nostro Istituto si impegna a creare dei momenti di condivisione in ingresso sulle tematiche relative alle TIC.
A tal proposito sia il Regolamento scolastico che il Patto di corresponsabilità saranno aggiornati con espliciti riferimenti alle TIC e all'ePolicy.

Il nostro piano d'azioni

AZIONI (da sviluppare entro un'annualità scolastica)

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

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

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo 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.

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.

Il diritto alla protezione dei dati personali e al ricevere un'adeguata istruzione sono due diritti che vanno coordinati e integrati.

Anche il CPIA BAT si è confrontato in materia di privacy attraverso un corso di formazione apposito rivolto a tutto il personale scolastico, relativo all'entrata in vigore del Regolamento UE 679/2016 (cosiddetto GDPR) e del successivo D.lgs. 10 agosto 2018, n. 101 che ha modificato il D.lgs. 196/2003 (cosiddetto Codice Privacy).

In particolare, la scuola, oltre a tutelare la privacy degli/lle studenti/esse e delle loro famiglie, si assumerà il compito di informare e soprattutto rendere consapevoli gli/le studenti/esse di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri.

Alcune categorie di dati personali degli/lle studenti/esse e delle famiglie, come quelli sensibili e giudiziari, saranno trattate con estrema cautela, nel rispetto di specifiche norme di legge, verificando in primis non solo la pertinenza e completezza dei dati, ma anche la loro indispensabilità rispetto alle "finalità di rilevante interesse pubblico" che si intendono perseguire.

Per le ragioni pocanzi esposte, il CPIA BAT avrà cura di tutelare la privacy di tutti i propri corsisti: ricordiamo che tra la sua utenza di allievi si annoverano anche ristretti della Casa Circondariale, dunque è d'obbligo tutelare anche la privacy delle persone in relazione alla loro situazione interpersonale giudiziaria e luogo di residenza temporaneo.

La scuola, informerà (tramite apposita informativa) tutti gli interessati delle caratteristiche e modalità del trattamento dei loro dati, indicando i responsabili del trattamento.

Il primo step che la scuola considererà sarà l'individuazione delle responsabilità. In primo luogo, si avrà cura di distinguere i soggetti che trattano dati personali da coloro i quali non sono autorizzati ad accedere ai dati e, nell'ambito dei soggetti autorizzati a trattare i dati, individuare i referenti preposti alla gestione delle diverse procedure. In quest'ottica, saranno pensati piani di formazione differenziati a seconda della responsabilità aziendale che riveste il soggetto autorizzato e dei trattamenti che questi effettua sotto l'autorità del titolare.

In secondo luogo si procederà alla gestione efficiente dei registri, utilizzando quattro tipi di modelli fra cui il registro delle attività di trattamento, il registro per la gestione delle violazioni, il registro della formazione e, da ultimo, il registro della

strumentazione.

Si ricorda, inoltre, che il nostro Istituto ha già individuato la figura del Data Protection Officer (DPO) come previsto dal Regolamento Ue 679/2016.

I punti fondamentali che il CPIA BAT soddisferà riguarderanno i riferimenti al citato Regolamento quali:

1.Redigere e mantenere un registro dei trattamenti dei dati: sia per il titolare che per il responsabile dei trattamenti.

2.Valutazione dei rischi sulla privacy: (definita nel regolamento Data Protection Impact Assessment o PIA) relativamente ad alcune tipologie di trattamento dei dati sensibili. Le istituzioni scolastiche pubbliche e private possono trattare anche dati sensibili, come ad esempio dati relativi alle origini razziali per favorire l'integrazione degli/lle alunni/e, dati relativi alle convinzioni religiose, al fine di garantire la libertà di culto, e dati relativi alla salute per adottare misure di sostegno degli/lle alunni/e, come i dati vaccinali con le Asl.

3.Analisi di processo sulla raccolta/gestione del consenso: occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio, all'interno di modulistica o sul proprio sito web istituzionale. Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice e chiara (art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali, ma devono ad esempio adeguare tutta la modulistica al Regolamento UE 2016/679 e predisporre una lettera di incarico per il trattamento dei dati al personale ATA, ai collaboratori scolastici e ai docenti.

4.Adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti.

5.Analisi del sito web istituzionale di riferimento con proposte volte a migliorare la sicurezza e la protezione dei dati trattati.

6. Proposte di messa in sicurezza della rete intranet scolastica.

Infine come stabilito dal Garante per la protezione dei dati personali, la scuola renderà noto alle famiglie e ai ragazzi, attraverso un'adeguata informativa, quali dati raccolgono e come li utilizzano. I modelli di liberatoria che l'Istituto adopererà o intende utilizzare, saranno modelli conformi alla normativa vigente, in materia di protezione dei dati personali.

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.

Il ruolo delle nuove tecnologie dell'informazione e della comunicazione nel sistema dell'Istruzione degli Adulti è individuato come centrale già nelle Linee Guida per il passaggio al nuovo ordinamento dei CPIA regolamentato dal DPR 263/2012.

Ben prima che l'emergenza pandemica ci abituasse a sigle come DAD e DDI, proprio l'utilizzo delle ICT già contemplava la Fruizione a Distanza (FAD) come una delle principali innovazioni dell'assetto organizzativo e didattico dell'Istruzione degli Adulti, con il triplice obiettivo di sviluppare le competenze digitali degli studenti, favorire la personalizzazione dei percorsi, offrire una concreta opportunità per la flessibilità nella

frequenza.

Sulla base di queste premesse e di un percorso che ha visto protagonista la RIDAP con il gruppo nazionale di formazione sull'innovazione didattica, è maturata l'idea di costituire una rete di scopo sui temi delle ICT, con la finalità di individuare obiettivi e linee operative, fornire carattere strutturale alle azioni, favorire lo sviluppo di comunità di pratiche, reinterpretare le previsioni del DPR 263/12 nell'ottica più ampia della Didattica Digitale Integrata.

Alla Rete di scopo ICT IdA della RIDAP hanno aderito 23 CPIA distribuiti su tutto il territorio nazionale tra cui il CPIA BAT.

In linea con le disposizioni sopra elencate e tenuto conto che i nostri corsisti necessitano di approcci maggiormente individualizzati in relazione alle caratteristiche di ognuno di loro in quanto adulti, il nostro Istituto si è impegnato a stimolare un uso consapevole e responsabile degli strumenti digitali e delle nuove tecnologie in modo da:

- saper utilizzare i dispositivi digitali nel rispetto dei regolamenti dell'Istituto, solo per fini didattici e su autorizzazione esplicita e motivata dell'insegnante;
- offrire iniziative in presenza e a distanza per il recupero degli apprendimenti e delle altre situazioni di svantaggio determinate anche dalla recente emergenza sanitaria;
- intraprendere azioni di formazione e aggiornamento del personale scolastico in tema di competenze digitali al fine di implementare e consolidare pratiche didattiche efficaci con l'uso delle nuove tecnologie, utili anche nei periodi di emergenza sanitaria, a supporto degli apprendimenti delle studentesse e degli studenti.

Come stabilito dal Piano Nazionale Scuola Digitale (PNSD), secondo le previsioni dell'AZIONE N° 28, il CPIA BAT ha istituito la figura dell'animatore digitale nell'ambito del proprio organico docenti di ruolo, con relativa formazione per quest'ultimo attraverso un percorso dedicato su tutti i temi del Piano Nazionale Scuola Digitale.

Per tenere alta l'attenzione sui temi dell'innovazione, nell'ambito della realizzazione delle azioni previste nel POF triennale, l'animatore digitale potrà sviluppare la progettualità su tre ambiti: formazione interna, coinvolgimento della comunità scolastica, organizzazione di soluzioni innovative.

Il piano di intervento si fonda inoltre su temi strutturali, quali:

- la formazione di base di tutto il corpo docente sull'uso degli strumenti per la didattica e la formazione specifica dell'Animatore Digitale;

- la segnalazione di eventi formativi, concorsi e bandi nell'ambito del PNSD;

- la ricognizione della connettività e delle dotazioni tecnologiche nelle varie Sedi

Associate e Punti di Erogazione del Servizio;

- il sostegno alla Didattica Digitale Integrata;

- la pubblicizzazione delle attività svolte nell'ambito del PNSD.

Si prevede l'adozione di uno sportello permanente di assistenza, per rispondere alle diverse esigenze di docenti, studenti e altre figure coinvolte nel processo di digitalizzazione.

Con l'ePolicy il nostro Istituto si sta dotando di un regolamento sull'uso delle TIC che preveda una sezione dedicata all'uso di Internet, in cui gli studenti si impegnano a:

- utilizzare la rete nel modo corretto;
- rispettare le consegne dei docenti;
- non scaricare materiali e software senza autorizzazione;
- non utilizzare unità removibili personali senza autorizzazione;
- tenere spento lo smartphone al di fuori delle attività didattiche che ne prevedano l'utilizzo;
- durante le attività che prevedono lo smartphone, utilizzarlo esclusivamente per svolgere le attività didattiche previste;
- segnalare immediatamente materiali inadeguati ai propri insegnanti.

I docenti si impegnano a:

- utilizzare la rete nel modo corretto;
- non utilizzare device personali se non per uso didattico;
- formare gli studenti all'uso della rete;
- dare consegne chiare e definire gli obiettivi delle attività;
- monitorare l'uso che gli studenti fanno delle tecnologie a scuola.

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.

D'altro canto, grazie agli strumenti di comunicazione online, come già in parte sottolineato, possiamo usufruire dell'interattività del mezzo, superare le barriere

spazio-temporali, usare un linguaggio multimediale, ipertestuale e accattivante, promuovere la partecipazione e il coinvolgimento dei diversi attori in gioco nel processo educativo.

In linea con l'ePolicy, il CPIA BAT ha adottato diversi canali di comunicazione per il proprio personale scolastico, allievi e famiglie.

La comunicazione con i corsisti avviene tramite una piattaforma esterna (Agorà), collegata al Registro Elettronico, utilizzata per la didattica a distanza: essa permette agli allievi la connessione da remoto ed assistere a videolezioni di ogni disciplina, oltre all'inserimento di compiti a distanza multimediali (video, foto, articoli per il sito, documenti, elaborati anche di gruppo).

Fra i vari strumenti di comunicazione, il CPIA BAT utilizza il Registro Elettronico, consentendo la visualizzazione di molte informazioni utili ai corsisti e alle famiglie degli studenti minorenni, tra cui:

- andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari);
- risultati scolastici (voti, documenti di valutazione);
- prenotazioni colloqui individuali;
- lettura di circolari;
- eventi (agenda eventi);
- comunicazione varie (comunicazioni di classe, comunicazioni personali).

Oltre al Registro Elettronico, un fondamentale canale di comunicazione online è il sito istituzionale (raggiungibile all'indirizzo https://www.cpiabat.edu.it/), costantemente aggiornato con avvisi, circolari ed eventi in evidenza: nel sito sono facilmente reperibili i contatti del Dirigente Scolastico, della segreteria, dei referenti di plesso.
Recentemente il CPIA BAT si è anche dotato di una pagina Facebook istituzionale (Pagina Facebook del CPIA BAT) e di un proprio canale YouTube (Canale YouTube del CPIA BAT)

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.

La questione, affrontata per la prima volta in maniera integrata nel Piano Nazionale Scuola Digitale emanato dal Miur con la Legge 107 del 2015, pone l'attenzione verso le tecnologie digitali e il loro utilizzo in classe e le stesse vengono riproposte come strumenti da inserire nella didattica e nelle sperimentazioni laboratoriali. L'uso viene consentito per scopi prettamente didattici, sotto il controllo e la responsabilità del docente che pianifica l'attività didattica.

Il CPIA BAT, al fine di garantire una didattica digitale innovativa e sicura, si è dotato di strumenti digitali presso tutte le proprie Sedi Associate e PES (LIM, tablet, computer, monitor multimediali), per consentire ai propri corsisti una lezione più interattiva e partecipata, compresi i ristretti della Casa Circondariale di Trani.

Inoltre, anche in considerazione dell'emergenza sanitaria dovuta al COVID-19, visto il Decreto del Ministero dell'Istruzione n.187 del 26/03/2020 recante istruzione in merito all'articolo 120, comma 5 del D.L. n. 18 del 17.03.2020, il nostro Istituto ha avuto la possibilità di ricevere dispositivi digitali e strumenti per la connettività individuali, in modo da consentire la fruizione delle piattaforme per la didattica a distanza, da mettere a disposizione degli studenti meno abbienti in comodato d'uso gratuito. Terminata la fase di emergenza sanitaria, questi strumenti saranno sempre a disposizione dei corsisti, sia per le attività in aula che per il comodato d'uso gratuito.

I dispositivi digitali individuali sono consegnati previa sottoscrizione di un contratto di comodato con relativa assunzione di responsabilità e dovranno essere restituiti perfettamente funzionanti, completi dell'imballo originario integrale, all'ufficio di segreteria della Scuola.

All'atto della richiesta, il richiedente dichiara:

- di rientrare nelle casistiche previste nel D.L. 18 del 17.03.2020;
- di disporre di accesso a internet sufficiente per supportare la Didattica a Distanza (altrimenti si dovrebbe provvedere con ulteriore strumento per la connettività individuale);
- di NON aver presentato né di voler presentare analoga richiesta ad altre istituzioni scolastiche;
- di NON aver ricevuto o di NON ricevere dispositivi a seguito di altre iniziative di solidarietà digitale.

Inoltre, il richiedente si impegna a far rispettare o/a rispettare le seguenti regole di utilizzo del dispositivo digitale:

- lo studente può utilizzare il dispositivo durante le ore di lezione e, al di fuori, esclusivamente per usi e scopi didattici, secondo le indicazioni dei vigenti regolamenti e/o fornite dagli Insegnanti;
- è vietato l'utilizzo dell'apparecchio per qualunque altra attività non autorizzata dal Docente;
- lo studente non può effettuare download di proprietà, gratuiti e a pagamento senza apposita autorizzazione da parte del Docente;
- è vietato effettuare qualsiasi modifica non autorizzata ai sistemi operativi, che potrebbe interferire generando incompatibilità con i dispositivi utilizzati e condivisi dal gruppo classe;
- lo studente deve provvedere a mantenere in efficienza il dispositivo per l'uso didattico e averne cura per tutta la durata del comodato d'uso;
- la responsabilità di eventuali danni al dispositivo, durante il periodo di concessione, è in capo al richiedente.

Il richiedente è consapevole che ogni violazione delle suddette regole, comporterà il ritiro immediato del dispositivo, con riserva di provvedimenti disciplinari o di segnalazioni alle Autorità.

I dati raccolti sono acquisiti e trattati per i fini istituzionali previsti dalla Legge e dai regolamenti, nel rispetto del Regolamento UE n. 679/2016 (GDPR); la raccolta dei dati è obbligatoria per la fase istruttoria dei procedimenti amministrativi correlati e per il corretto sviluppo dell'azione amministrativa.

Il Titolare del trattamento dei dati è il CPIA-BAT, in persona del Dirigente Scolastico.

Inoltre la scuola ha disposto, secondo l'artico 3 del D.P.R. n. 249/1998, "per ciascuno studente, di non utilizzare il telefono cellulare, o altri dispositivi elettronici, durante lo svolgimento delle attività didattiche" secondo le seguenti disposizioni interne:

1. Nei locali della scuola salvo specifica autorizzazione del Dirigente Scolastico o suo delegato lo stesso deve essere tenuto spento, con tutte le funzioni disattivate e non in vista;
2. L'uso del cellulare può essere concesso in deroga alla normativa vigente, solo ai frequentanti adulti che abbiano particolari esigenze (ad esempio: reperibilità lavorativa, seri motivi di famiglia, ecc.). In caso di necessità è comunque richiesto l'uso della suoneria in modalità silenziosa. L'utente avrà cura di uscire dall'aula qualora sopraggiungessero impellenti necessità di comunicare con l'esterno;
3. La stessa norma si applica ad altri dispositivi elettronici (tablet, lettori mp3/mp4 ecc.) il cui uso non sia stato espressamente autorizzato dal docente per lo svolgimento di un'attività didattica;
4. È vietato accendere il telefono cellulare nei locali della scuola;

5. I docenti possono ritirare il cellulare agli studenti che non rispettino il regolamento riconsegnandolo prima dell'uscita; lo studente ha il diritto di estrarre la scheda dal proprio cellulare per tutela della propria privacy;
6. È assolutamente vietato pubblicare fotografie e/o video senza il consenso degli interessati (dei genitori per i minori). La pubblicazione priva si consenso determina violazioni di tipo amministrativo e/o penale.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco di un'annualità scolastica).

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA

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

- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

I rischi online rappresentano tutte quelle situazioni problematiche derivanti da un uso non consapevole e non responsabile delle tecnologie digitali da parte di ragazzi e ragazze: adescamento online, cyberbullismo, sexting, violazione della privacy, pornografia, pedopornografia, gioco d'azzardo o gambling, internet addiction, videogiochi online, esposizione a contenuti dannosi o inadeguati. Partendo da questo

punto di vista, vanno promosse nei più giovani le necessarie competenze e capacità, al fine di una protezione adeguata, ma anche al fine di un utilizzo consapevole che sappia sfruttare le potenzialità delle tecnologie digitali e gestirne le implicazioni.

Il concetto di prevenzione nasce in ambito epidemiologico e, seguendo quanto riportato dal Ministero della Salute, si può sintetizzare come un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere e conservare lo stato di salute ed evitare l'insorgenza di malattie.

Il CPIA BAT, come prevenzione in ambito digitale, organizzerà un insieme di attività, azioni ed interventi con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di ragazze/i.

Se il problema della "sicurezza" è difficilmente riconducibile esclusivamente all'esistenza in sé di alcuni rischi, più o meno gravi e insidiosi, appare chiaro dunque come le migliori strategie di intervento siano di carattere prevalentemente preventivo per consolidare quelle competenze educative di base necessarie a poter gestire le situazioni di vita che i/le ragazzi/e sperimentano online.

Come sappiamo, le dimensioni che il fenomeno coinvolge sono molteplici e non puramente tecniche e si rifanno alla capacità dei più giovani di gestire situazioni complesse che richiedono:

- la capacità di gestire la relazione con l'altro/a diverso/a da sé;
- le dimensioni dell'affettività e della sessualità;
- il riconoscimento di un limite, anche, ma non solo, correlato ad una dimensione di legalità;
- l'utilizzo sicuro e consapevole delle tecnologie digitali.

Per questo motivo la scuola deve rafforzare la sua capacità di rispondere anche a questi bisogni attraverso strumenti e misure specifiche. Allo stesso modo, quando un evento problematico connesso ai rischi online coinvolge il contesto scolastico, è fondamentale per la scuola poter dare una risposta il più possibile integrata, che trovi la sua espressione di indirizzo in procedure chiare di cui deve dotarsi e che includano la collaborazione (prevedendo accordi specifici) con la rete dei servizi locali (in primis le ASL e la Polizia Postale).

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

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

La stessa legge e le relative **Linee di orientamento per la prevenzione e il contrasto del cyberbullismo** indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

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

Il Dirigente Scolastico qualora venga a conoscenza di atti di cyberbullismo informerà tempestivamente i genitori dei minori coinvolti (L. 71/2017, art.5).

Un'indicazione operativa da tener presente per intervenire efficacemente è anche capire se si tratti 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. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza.

Per quanto riguarda la necessità di segnalazione e rimozione, 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 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. Il Garante ha pubblicato nel proprio sito il modello per la segnalazione/reclamo in materia di cyberbullismo da inviare a: cyberbullismo@gpdp.it.

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

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

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.

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

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

Il CPIA BAT nell’ambito dell’educazione civica affronterà i seguenti temi:

- il discorso dell’odio online
- i diritti umani
- la libertà di espressione
- il razzismo e la discriminazione
- vita privata e sicurezza
- democrazia e partecipazione

La mission del CPIA BAT, così come indicato nel PTOF, è finalizzata prioritariamente all’educazione e all’istruzione delle persone con maggiori fragilità socioculturali: ragazzi minorenni e adulti italiani e stranieri, persone che nei paesi d’origine non hanno avuto accesso all’istruzione, stranieri richiedenti asilo, persone in esecuzione penale esterna o agli arresti domiciliari, minoranze etniche.
Proprio per questo la nostra Istituzione scolastica pone costantemente al centro della propria azione educativa tematiche come l'integrazione e la lotta ad ogni forma di discriminazione.

Saranno organizzati eventi di sensibilizzazione, contattando le organizzazioni locali attive contro il razzismo e la discriminazione o altri problemi correlati per affrontare le seguenti tematiche:

- il problema generale del discorso dell'odio online
- i pregiudizi su un particolare gruppo preso di mira
- i metodi di lotta contro il discorso dell'odio
- l'impatto del discorso dell'odio
- la necessità che la gente assuma responsabilità per le proprie azioni e per quelle degli altri
- le iniziative intraprese da altri gruppi di giovani, tra cui il No Hate Speech Movement

Inoltre il CPIA BAT organizzerà corsi di alfabetizzazione digitale, intesa come la capacità di accedere a Internet, di comprendere, analizzare criticamente e creare informazioni e contenuti online. In generale, ogni utente di Internet impara i metodi e le norme necessari per navigare online nel corso delle sue attività in rete: diventa così sufficientemente "competente" nel campo di Internet per riuscire a cavarsela da solo e soddisfare la maggior parte delle sue esigenze. Tuttavia, se si vuole evitare che i giovani riproducano alcuni degli aspetti negativi e certe cattive abitudini che sono la conseguenza del discorso dell'odio online, e, in particolare, se si vuole che imparino ad affrontare delle situazioni particolari, diventa necessaria una maggiore padronanza di Internet.

4.4 - Dipendenza da Internet e gioco online

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

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

La scuola ha la possibilità di fare formazione e di indicare strategie per un uso più consapevole delle tecnologie per favorire il "benessere digitale", cioè la capacità di creare e mantenere una relazione sana con la tecnologia. La tecnologia infatti ha modificato gli ambienti che viviamo e ha un impatto sulla qualità della vita. 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).

Questo è un argomento trasversale, se ne può parlare quando si parla di cittadinanza digitale, di cyberbullismo, di uso integrativo e non sostitutivo dei dispositivi e della Rete; tanto più può essere utile dedicare al tema un momento specifico e riflettere con studenti e studentesse per fare in modo che la tecnologia sia strumento per raggiungere i propri obiettivi e non sia solo distrazione o addirittura ostacolo.

IL CPIA BAT può insegnare molto da questo punto di vista se integra la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online.

Se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi. L'intento è strutturare regole condivise con i corsisti e stipulare con loro una sorta di "patto" d'aula, oltre a proporre delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d'aula (Es. adoperando la LIM o il dispositivo personale BYOD). È importante, quindi, non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli/lle studenti e delle studentesse, stabilendo chiare e semplici regole di utilizzo.

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.

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 (la Legge 19 luglio 2019 n. 69, all'articolo 10 ha introdotto in Italia il reato di revenge porn, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti. Si veda l'articolo 612 ter del codice penale rubricato "Diffusione illecita di immagini o video sessualmente espliciti". 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.

E' auspicabile che il CPIA BAT organizzi periodicamente degli incontri con psicologi,

esperti del diritto (magistrati, avvocati penalisti) aperti ai genitori dei corsisti minorenni, al fine di mettere in guardia gli allievi sui rischi penali a cui vanno incontro nella diffusione di immagini dal contenuto sessualmente esplicito. Ciò al fine di evitare che sull'alunno possa gravare un procedimento penale per diffusione anche inconsapevole di materiale pedopornografico.

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.

Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e della sessualità.

Fondamentale quindi, come sappiamo, 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.

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, se si ravvisa un rischio per il benessere psicofisico dei ragazzi/e coinvolte 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; Polizia di Stato – Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza. I più giovani devono acquisire quelle competenze in grado di orientarli e guidarli nelle loro scelte anche online; per questo motivo, come già sottolineato, l'educazione, compresa l'educazione all'affettività, riveste un ruolo fondamentale.

Il nostro piano d'azioni

AZIONI (da sviluppare entro un'annualità scolastica).

- 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 di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli 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.

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.

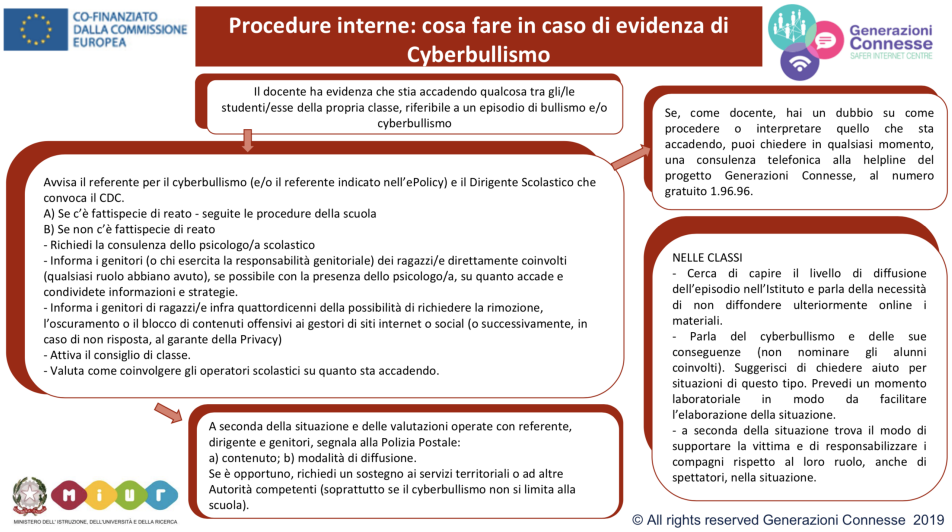
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **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.

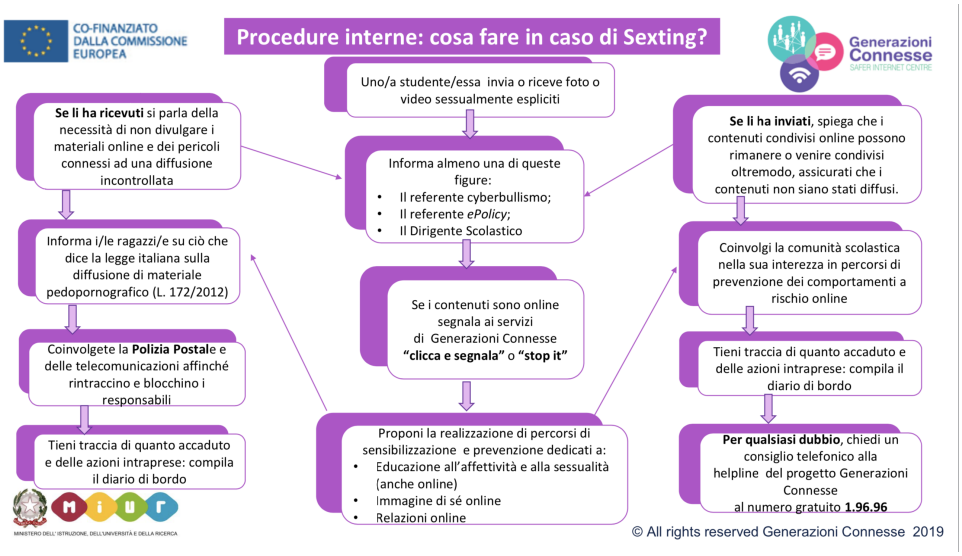
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

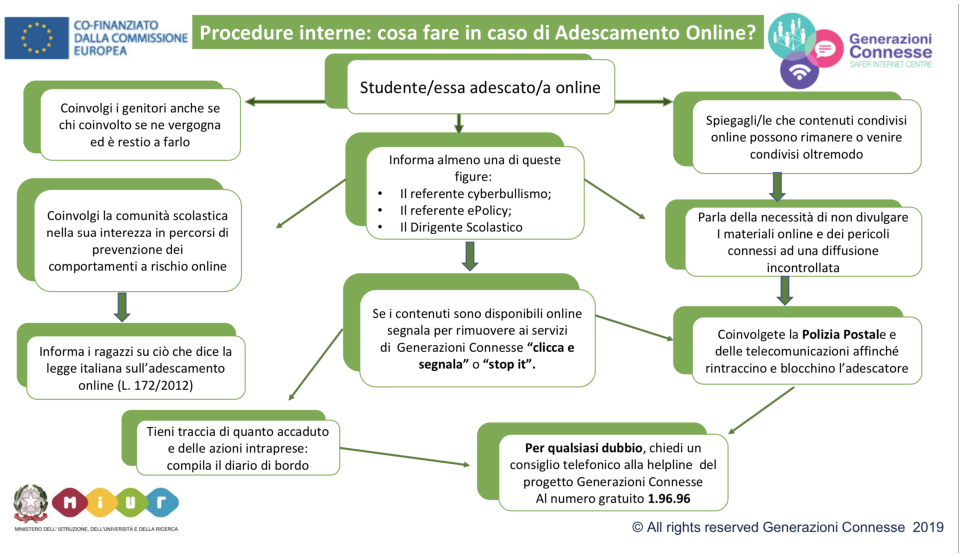
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



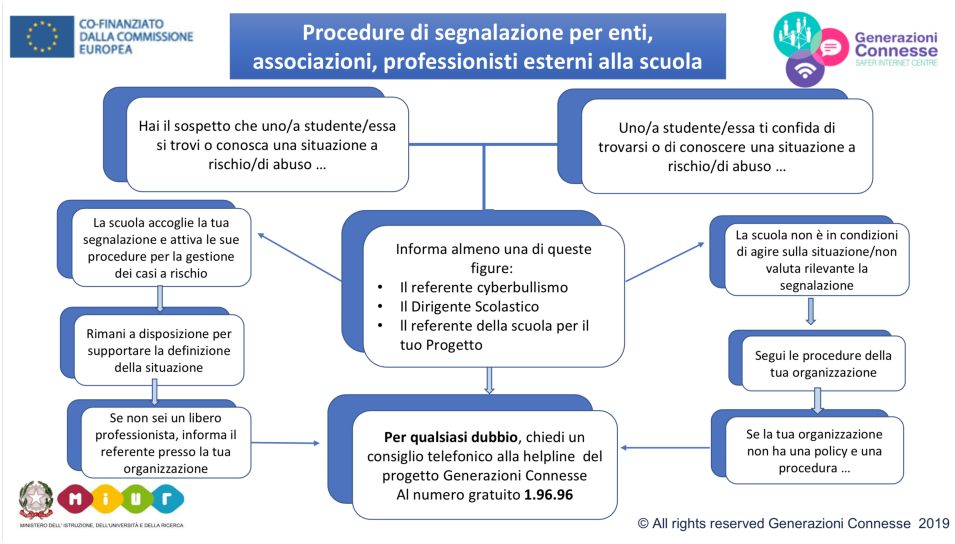
Procedure interne: cosa fare in caso di sexting?



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.

PAOLO FARINA
17.09.2021 07:59:53 UTC