Documento di ePolicy

TOIC8AC00D

I.C. RIVAROLO C.SE

VIA LE MAIRE 20 - 10086 - RIVAROLO CANAVESE - TORINO (TO)

Brunella Buscemi

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.

Sia a livello internazionale, sia nel contesto italiano, la presenza sempre più diffusa delle tecnologie digitali nella vita quotidiana delle nuove generazioni apre a molte opportunità, ma pone nuove attenzioni dal punto di vista del loro uso sicuro, consapevole e positivo.

La scuola, in virtù del gravoso compito di educare, non può negare tale evidenza e non può sottrarsi dal farsi carico della responsabilità pedagogica nei confronti dei propri alunni.

L'insegnamento, l'apprendimento e il consolidamento delle competenze digitali sono un obiettivo stabilito dal Piano Nazionale Scuola Digitali (DM. N.851/2015). Secondo questo indirizzo ciò permetterebbe agli alunni, futuri cittadini, l'uso proficuo, consapevole e responsabile della tecnologia, e al contempo un'evoluzione positiva della dinamica insegnamento/apprendimento sempre più contestualizzata all'ambito del reale.

E-Safer Policy è una policy di sicurezza TIC che consente di identificare le regole e le procedure per tutti gli utenti che utilizzano le risorse, il patrimonio TIC e l'accesso alla rete internet dell'Istituto Comprensivo, e tiene in debita considerazione quanto previsto dal Piano di Azione.

La Policy è un documento programmatico che impegnerà l'Istituto Comprensivo di Rivarolo anche per gli anni futuri. Da ciò ne consegue che quanto descritto nel seguito verrà realizzato nel corso del prossimo triennio. Durante tale periodo, verranno monitorati gli esiti rispetto alle attese prefissate, e, in ragione dei risultati ottenuti in itinere, il presente documento sarà oggetto di ampliamento e modifica, tenendo anche in considerazione gli sviluppi contestuali e le indicazioni fornite dalle agenzie preposte.

L' Istituto Comprensivo di Rivarolo, nell'elaborare il Piano di Azione, ha eseguito una valutazione dei rischi a cui possono essere esposti i propri alunni considerando la particolare fascia di età di questi ultimi.

Nello specifico, il gruppo di lavoro, tenendo conto delle indicazioni fornite dagli organi di Polizia e dalle Istituzioni che collaborano alla prevenzione del fenomeno del bullismo, cyberbullismo e affini, ha individuato tre aree di rischio:

- Contenuti:
    - Esposizione a contenuti dannosi e non appropriati
    - Siti web che promuovono stili di vita e comportamenti dannosi
    - Contenuti che spingono all'odio

    - Contenuti mendaci
    - Pornografia
- Contatto:
    - Grooming (adescamento online), sfruttamento sessuale
    - Cyberbullismo e bullismo in tutte le forme
    - Furto di identità
    - Pedopornografia
- Condotta:
    - Comportamenti aggressivi
    - Violazione della privacy e divulgazione di dati personali
    - Reputazione digitale
    - Dipendenze da internet
    - Eccesso d'uso di videogiochi
    - Sexting
    - Violazione del copyright

Il presente documento ha il duplice scopo di prevenire e gestire situazioni problematiche relative all'uso di tecnologie digitali e facilitare e promuovere l'utilizzo positivo delle TIC (Tecnologie dell'Informazione e Comunicazione) nella didattica e negli ambienti scolastici dell'Istituto Comprensivo di Rivarolo. Nello specifico gli scopi del presente documento sono così riassumibili:

- definire i principi fondamentali condivisi da tutti i membri della comunità scolastica rispetto all'uso delle TIC,
- salvaguardare e proteggere i bambini, i ragazzi e tutto il personale dall'uso improprio delle TIC e dai soggetti che le utilizzano in modo deviato,
- assistere il personale della scuola nel lavorare in modo sicuro e responsabile con le TIC,
- monitorare i propri standard e le prassi,
- definire chiare aspettative di comportamento per un uso responsabile della rete Internet, sia in ambito didattico sia al di fuori di tale contesto,
- avere procedure chiare per affrontare l'uso improprio degli strumenti digitali o gli abusi online,
- assicurarsi che tutti i membri della comunità scolastica siano consapevoli che i comportamenti illeciti o pericolosi sono inaccettabili e sanzionati a norma del Regolamento di Istituto e della legislazione vigente.

La presente Policy si applica a tutta la comunità scolastica dell'Istituto Comprensivo di Rivarolo. Nello specifico è rivolta:

- ai bambini, che frequentano la scuola dell'Infanzia e la scuola Primaria;
- ai ragazzi della Secondaria di Primo Grado;
- a tutto il personale docente che svolge la sua attività di insegnamento nei plessi dell'Istituto Comprensivo, anche per brevi periodi;
- al Dirigente Scolastico (DS) e al Dirigente dei Servizi Generali e Amministrativi (DSGA);

- a tutto il personale amministrativo e a tutti i collaboratori scolastici (ATA);
- a tutti gli operatori/professionisti e/o volontari che entrano a scuola;
- ai genitori e famiglie degli alunni;
- ai visitatori/ospiti;
- a tutti coloro che hanno accesso ai sistemi di connessione e usano qualsiasi strumentazione digitale della scuola o anche dispositivi personali dentro e fuori dall'Istituto Comprensivo.

1.2 - Ruoli e responsabilità

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

Il referente d'Istituto per la prevenzione al bullismo e cyberbullismo (più avanti solo Referente d'Istituto – nominato secondo le disposizioni della L. 107/2017), in collaborazione con l'Animatore Digitale, assistiti dal Team per l'innovazione tecnologica, hanno la funzione di coordinare le attività descritte nella presente Policy in accordo con quanto definito nel Piano di Azione, di aggiornarla annualmente (se necessario), di presentarla al Collegio ad ogni inizio di anno scolastico e renderla pubblica attraverso gli organi di informazione di cui è dotata la scuola (es. sito web istituzionale) e durante gli incontri e i momenti di incontro con gli alunni in ingresso.

Le due figure succitate hanno altresì la funzione di monitorare l'applicazione della Policy da parte dei colleghi docenti e del personale ATA riferendo eventuali problemi al Dirigente Scolastico, mentre ciascun insegnante ha la responsabilità di monitorarne l'applicazione da parte dei propri studenti.

È in capo al Referente d'Istituto, sentito l'Animatore Digitale, il Team Digitale e gli altri organi collegiali preposti e il Gruppo di Lavoro per l'Inclusività (GLI), proporre e incentivare le attività di formazione e informazione per gli alunni che hanno come obiettivo la prevenzione dei casi di bullismo, cyberbullismo, sexting, violazione della privacy, adescamento, pedopornografia.

La rilevazione dei casi avviene durante la normale attività dei docenti curricolari, del Referente d'Istituto, dell'Animatore Digitale, dello sportello di ascolto e del personale ATA in servizio presso la scuola, e più in generale di tutto il personale professionale che svolge un'attività continuativa e inquadrata nell'organigramma scolastico (es. psicologo dello sportello di ascolto).

In caso di segnalazione, il personale scolastico (docente, ATA, educatori, ecc) avrà come primo interlocutore il Referente d'Istituto, il quale informerà tempestivamente il

Dirigente Scolastico (o in sua assenza/impossibilità il Vicario) dell'accaduto.

All'interno dell'Istituto Comprensivo di Rivarolo è ammesso solo l'uso di strumenti informatici (mobile e fissi) in modalità cablata e/o WiFi di proprietà dello stesso Istituto Comprensivo.

Nel caso specifico del personale docente e ATA, è loro permesso l'impiego di dispositivi propri (smartphone, tablet, notebook) purché finalizzato allo svolgimento delle attività scolastiche (didattiche, organizzative, ecc).

Agli alunni è sempre fatto divieto d'usare i dispositivi propri (connessi e non connessi) entro le aree comuni esterne ed interne del plesso scolastico, le aule e i laboratori.

Nello specifico si evidenziano nel seguito le responsabilità chiave per i principali soggetti coinvolti nell'applicazione delle Policy.

- Dirigente Scolastico e DSGA:
    - deve essere adeguatamente formato sulla sicurezza e prevenzione di problematiche offline e online, in linea con le leggi di riferimento e i suggerimenti del MIUR e delle sue agenzie;
    - deve promuovere la cultura della sicurezza online, integrandola ed inserendola nelle misure di sicurezza più generali dell'intero Istituto;
    - ha la responsabilità della gestione dei dati e della sicurezza delle informazioni e garantisce l'utilizzo delle corrette procedure di trattamento dei dati personali;
    - ha il compito di garantire a tutto il personale una formazione adeguata sulla sicurezza online per essere tutelato nell'esercizio del proprio ruolo educativo e non;
    - deve essere a conoscenza delle procedure da seguire in caso di un grave incidente di sicurezza online.
- Team Digitale:
    - si fa carico giorno per giorno dei problemi di sicurezza online e sono riferimento per la creazione e la revisione delle politiche di sicurezza online della scuola e dei relativi documenti;
    - si impegna a promuovere la cultura della sicurezza on-line in tutta la comunità scolastica;
    - garantiscono che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente di sicurezza on-line;
    - collaborano, in base alle necessità, con il personale tecnico esterno per il raggiungimento degli obiettivi di sicurezza previsti dalla Policy.
- Referente d'Istituto per il bullismo e cyberbullismo:
    - supporta il Dirigente Scolastico e il personale scolastico nella gestione delle segnalazioni di casi;
    - coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo per il personale scolastico, alunni e famiglie;

- collabora con le Forze di Polizia e con le associazioni e i centri di aggregazione giovanile del territorio.

- Animatore Digitale:
  - garantisce che l'uso della TIC della scuola e le piattaforme online dell'Istituto siano regolarmente monitorate e che qualsiasi abuso/uso improprio o qualsiasi tentativo relativo ad essi è segnalato al Dirigente Scolastico.
  - promuove la formazione tecnico-informatico del personale scolastico;
  - garantisce che l'educazione all'uso consapevole delle TIC e alla sicurezza online sia inserita all'interno del curricolo di studi dei bambini e dei ragazzi;
  - promuove la formazione del personale scolastico circa i rischi online, la protezione e gestione dei dati personali;
  - promuove percorsi di formazione interna all'Istituto nell'ambito dello sviluppo della "scuola digitale".
- Docente Responsabile di Laboratorio:
  - segnalano problemi relativi alla sicurezza online rilevati al DS e al Referente d'Istituto per il bullismo e cyberbullismo;
  - gestiscono i sistemi informatici della scuola, assicurando che:
    - la policy di sicurezza password sia rigorosamente rispettata;
    - tutti i sistemi per il rilevamento di usi impropri e di attacchi/minacce intenzionali siano attivi;
    - presso il plesso sia attivo e funzionale il sistema di web filtering.
  - si tengono aggiornati sulla policy di sicurezza online della scuola e condividono le informazioni tecniche al fine di svolgere efficacemente il proprio ruolo.
- Docenti:
  - leggono, approvano in sede collegiale e aderiscono alla presente Policy di utilizzo;
  - educano alla sicurezza online nello svolgersi del curriculum della propria disciplina;
  - supervisionano e guidano gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono tecnologie online;
  - garantiscono che gli alunni siano capaci di ricercare contenuti online in sicurezza e siano pienamente consapevoli dei problemi relativi ai contenuti elettronici (come ad esempio le leggi sul copyright).
  - segnalano al Referente d'Istituto e/o al Dirigente Scolastico qualsiasi abuso sospetto o accertato.
- Personale Tecnico, Amministrativo e Ausiliario:
  - devono leggere, comprendere, aderire alla presente Policy;
  - devono segnalare qualsiasi abuso sospetto o qualsiasi problema al Referente d'Istituto e/o al Dirigente Scolastico;
  - hanno consapevolezza delle problematiche di sicurezza online prese in esame dalla scuola con questo documento;

- assumono comportamenti sicuri, responsabili e professionali nell'uso delle tecnologie.

- Alunni:
  - leggono, capiscono, e aderiscono alla presente Policy;
  - capiscono l'importanza di segnalare l'abuso, l'uso improprio o l'accesso a materiali inappropriati;
  - sanno quali azioni intraprendere se loro o qualcuno che conoscono si sente preoccupato o vulnerabile quando utilizza la tecnologia online;
  - capiscono l'importanza di adottare sempre comportamenti sicuri e buone pratiche di sicurezza online quando usano le tecnologie digitali e sono consapevoli che la policy di sicurezza online della scuola può aiutarli anche fuori dalle mura e/o dall'orario scolastico.
- Genitori:
  - leggono, capiscono, e aderiscono alla presente Policy;
  - si consultano con il Referente d'Istituto, il Fiduciario di plesso e il Dirigente Scolastico se hanno preoccupazioni circa l'uso della tecnologia online o offline da parte dei loro figli;
  - sostengono la scuola nel promuovere la sicurezza online.

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).

Per i soggetti esterni che erogano attività educative nell'Istituto è ammesso l'uso dei dispostivi personali unicamente per l'assolvimento dei compiti assegnati e limitatamente allo svolgimento di tali attività. Nello specifico, i soggetti esterni:

- devono leggere, comprendere, aderire alla presente Policy;
- devono segnalare qualsiasi abuso sospetto o qualsiasi problema al Referente d'Istituto e/o al Dirigente Scolastico secondo le modalità indicate nel presente documento;
- hanno consapevolezza delle problematiche di sicurezza online prese in esame dalla scuola con questo documento;
- assumono comportamenti sicuri, responsabili e professionali nell'uso delle tecnologie.

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 Policy viene comunicata alla comunità scolastica e alle persone che usufruiscono dei servizi scolastici nei seguenti modi:

- sul sito dell'Istituto Comprensivo una volta approvata in modo definitivo;
- nelle bacheche degli spazi pubblici dei plessi;

- all’atto della nuova iscrizione (per alunni);
- all'atto di nuovo inserimento nel posto di lavoro (docenti, ATA);
- all'atto della sottoscrizione del contratto di collaborazione e/o erogazione di un servizio scolastico e di servizio da parte di fornitori/enti esterni;
- durante eventi e iniziative organizzate dall'Istituto nell'ambito della formazione/informazione di alunni, docenti e famgilie;
- durante le attività curricolari.

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.

L’Istituto Comprensivo di Rivarolo prenderà e manterrà nel tempo tutte le precauzioni necessarie per garantire agli alunni e al personale scolastico l'accesso sicuro ai contenuti digitali. Tuttavia, va precisato che dati i limiti umani e tecnologici, è di fatto impossibile per l’Istituto Comprensivo evitare in assoluto che gli alunni, durante le attività scolastiche che necessitano dell’uso delle TIC, possano imbattersi in contenuti inappropriati. In questo senso, l’Istituto Comprensivo non può farsi carico della responsabilità per il materiale trovato su internet o per eventuali conseguenze causate dall'accesso ad internet.

Qualora dovesse accadere un incidente, il Referente d’Istituto è la figura interna alla scuola che deve essere informata e allertata contestualmente al Fiduciario del plesso attraverso la compilazione del modulo digitale disponibile sul sito web dell'Istituto.

Qualsiasi sospetto, rischio, violazione evidenziati sulla popolazione studentesca vanno segnalati in giornata al Referente d’Istituto che a sua volta riferirà al Dirigente Scolastico. Qualsiasi allerta di uso improprio delle TIC, riferito al personale che a vario titolo presta servizio all’interno degli edifici scolastici, va sempre riferito direttamente al Dirigente Scolastico che procederà, in comune accordo con il DSGA, secondo quanto previsto dalla normativa vigente e dal CCNL.

In caso di infrazione alla Policy, il personale, gli alunni e gli altri componenti della comunità scolastica interessati verranno prontamente informati attraverso formale notifica del DS o del Vicario. Contestualmente verranno notificate le eventuali sanzioni.

Conformemente a quanto indicato nel Regolamento di Istituto, le sanzioni comminate agli alunni avranno carattere educativo/riabilitativo e in ogni caso verrà coinvolta la famiglia, in qualità di primi educatori.

Le infrazioni compiute dagli alunni considerate “di lieve entità” (secondo il giudizio del personale scolastico competente) verranno gestite dal Coordinatore della Classe (di concerto con il Consiglio di Classe) unitamente al Fiduciario del plesso scolastico in rapporto con il Referente d’Istituto (se necessario/utile di concerto con le Forze di Polizia o enti/associazioni di specialisti). Tali infrazioni verranno sanzionate come previsto dal Regolamento di Istituto.

Le infrazioni compiute dagli alunni considerate di comprovata gravità in realazione alla normativa vigente verranno gestite secondo quanto previste dalla normativa vigente. In questi casi il Dirigente Scolastico procederà a segnalare l'accaduto alle Forze di Polizia e agli organi preposti. Sarà cura del Responsabile di Istituto collaborare con il Dirigente Scolastico, le Forze di Polizia, gli specialisti esterni e il Consiglio di Classe per attivare un percorso educativo di assistenza e supporto per gli alunni coinvolti.

1.6 - Integrazione dell’ePolicy con Regolamenti esistenti

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

La ePolicy fa riferimento e si armonizza con tutti gli altri regolamenti vigenti nell'Istituto Comprensivo in particolare con il Regolamento di Istituto pertanto diventa vincolante per tutti i soggetti della comunità educante. Tutto ciò che qui non è normato è da considerarsi regolamentato secondo tale disciplina generale.

La Policy diventa parte integrante delle norme e dei regolamenti che l’Istituto Comprensivo autodefinisce nell’ambito dell’autonomia scolastica.

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.

La Policy sarà oggetto di riesame con cadenza annuale e/o al verificarsi di cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola e/o il recepimento delle nuove disposizioni normative nazionali.

Il gruppo di riesame e aggiornamento è composto dal Dirigente Scolastico, dal Team Digitale, dal Referente d'Istituto.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare un evento di presentazione del progetto Generazioni Connesse e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare un evento di presentazione del progetto Generazioni Connesse e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare strumenti di presentazione e divugazione del progetto Generazioni Connesse e conoscenza dell'ePolicy rivolti ai genitori
- Organizzare strumenti formativi/informativi per l'uso consapevole delle TIC per gli alunni
- Organizzare strumenti formativi/informativi per l'uso consapevole delle TIC per i docenti
- Organizzare strumenti formativi/informativi per l'uso consapevole delle TIC per le famiglie

Azioni da svolgere nei prossimi 3 anni:

- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy

rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori
- Organizzare eventi e iniziative per la formazione/informazione sull'uso consapevole delle TIC per alunni
- Organizzare eventi e iniziative per la formazione/informazione sull'uso consapevole delle TIC per docenti
- Organizzare eventi e iniziative per la formazione/informazione sull'uso consapevole delle TIC per famiglie

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.

Il curricolo verticale relativo alle competenze digitali è in corso di definizione puntuale. In linea generale sarà orientato al raggiungimento dei due obiettivi fondamentali:

- apprendere l'uso attento e responsabile delle TIC;
- responsabilizzare gli studenti davanti alla scelta dei comportamenti da assumere durante l'utilizzo delle TIC nei vari contesti d'impiego;

Per il raggiungimento di tali obiettivi, l'Istituto Comprensivo si avvarrà in modo strutturale delle risorse strumentali e professionali messe in campo dalla rete di ambito, dalla rete di scuole a cui appartiene, dagli Enti e Istituzioni presenti sul territorio, secondo quanto indicato nel Piano di Azione.

Nello specifico, il curriculm digitale, svilupperà si seguenti punti chiave:

- navigare, ricercare e filtrare dati, informazioni e contenuti digitali;
- valutare e gestire dati, informazioni e contenuti digitali;
- saper riconoscere e sapersi difendere da contenuti dannosi e pericolosi in Rete;
- saper interagire con gli altri attraverso le tecnologie digitali;
- essere consapevoli nella condivisione delle informazioni in Rete;
- essere buoni "cittadini digitali";
- collaborare adeguatamente con gli altri attraverso le tecnologie digitali;
- conoscere le "Netiquette";
- saper gestire la propria "identità digitale";
- creare e modificare contenuti digitali per esprimersi attraverso mezzi digitali;
- modificare, affinare, migliorare e integrare informazioni e contenuti all'interno di un corpus di conoscenze esistente per creare conoscenze e contenuti nuovi, originali e rilevanti;
- capire come il copyright e le licenze si applicano ai dati, alle informazioni e ai contenuti digitali;
- imparare a proteggere i dispositivi e i contenuti digitali e comprendere i rischi e le minacce presenti negli ambienti digitali;
- conoscere le misure di sicurezza e protezione e tenere in debita considerazione l'affidabilità e la privacy;
- proteggere i dati personali e la privacy negli ambienti digitali;
- conoscere (ed esercitare) i propri diritti in termini di privacy e sicurezza.

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

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

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

È compito del Team digitale analizzare in modo mirato il fabbisogno formativo dei colleghi docenti in materia di TIC, avviando specifici percorsi formativi aggiuntivi, distribuendo e condividendo il materiale informativo. A tal fine, verrà attivata un'apposita area del sito web istituzionale in cui rendere accessibili i documenti.

Indipendentemente dalla partecipazione alle iniziative di formazione, resta sempre attiva la disponibilità dell'Animatore Digitale, del Team Digitale e del Referente d'Istituto a fornire suggerimenti e consigli in materia di TIC e didattica.

Per la sensibilizzazione e formazione del personale ATA, soprattutto coloro che lavorano a stretto contatto con gli alunni, l'Istituto Comprensivo promuove la partecipazione dei dipendenti agli incontri e seminari organizzati dagli Enti e Uffici competenti.

Al fine di potenziare i momenti formativi, l'Istituto Comprensivo ha promosso la partecipazione dei docenti ai corsi di formazione nell'ambito della rete di scopo TO08, aventi per oggetto il miglioramento della competenza digitale.

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 rendere i propri docenti formati e informati sui temi all'oggetto della presente Policy, in particolare la sicurezza online, l'uso consapevole di Internet, l'emotività, la comunicazione ecc, l'Istituto Comprensivo di Rivarolo attiva una campagna informativa di sensibilizzazione per la partecipazione alle iniziative organizzate dall'Ufficio Scolastico Regionale, da altri enti e associazioni territoriali.

Quando possibile, sarà cura dell'Istituto Comprensivo organizzare internamente momenti formativi e informativi specifici anche con il contributo delle Forze di Polizia e enti/associazioni locali.

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.

A seguito della compilazione del Piano di Azione, l'Istituto Comprensivo si è attivato per sollecitare la partecipazione delle famiglie agli eventi di formazione e ai seminari organizzati dall'Ufficio Scolastico Regionale. Gli inviti vengono estesi con comunicazioni mirate.

È intenzione dell'Istituto Comprensivo continuare a informare le famiglie degli alunni circa i tempi e le modalità di svolgimento cercando di suscitare interesse. In contemporanea, l'Istituto cercherà, compatibilmente con le risorse finanziare disponibili, di organizzare al proprio interno momenti di condivisione e confronto con le famiglie sui temi all'oggetto della presente Policy. Tali interventi verranno prontamente promossi attraverso i canali informativi di Istituto.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco di una annualità)

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Promuovere per il corpo docente incontri formativi sull'utilizzo

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

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

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

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

Presso l'Istituto Comprensivo di Rivarolo sono in uso le seguenti pratiche atte a proteggere i dati personali:

- il responsabile del trattamento dei dati personali dell'Istituzione scolastica è il Dirigente Scolastico;
- il Dirigente Scolastico designa quali incaricati sono preposti al trattamento dei dati definendo i criteri di gestione;
- il personale incaricato è istruito sulla procedura da seguire per segnalare eventuali incidenti dove la protezione dei dati potrebbe essere stata compromessa.
- il personale scolastico viene ripetutamente formato e informato circa il trattamento dei dati personali mediante corsi di formazione.
- accettazione da parte del personale scolatico del regolamento sul trattamento dei dati personali.

Il personale incaricato della gestione dei dati personali ha un'area protetta sulla rete per memorizzare i file sensibili (segreteria digitale e registro elettronico). Al personale autorizzato viene richiesto di usare i sistemi di logout al momento di lasciare la postazione usata.

Gli uffici di segreteria sono dotati di mezzi elettronici adeguati ad impedire l'accesso dall'esterno alla rete, quali firewall od altri strumenti.

Presso l'Istituto Comprensivo di Rivarolo:

- viene chiesto esplicito permesso dei genitori/tutore legale per utilizzare fotografie digitali o video che coinvolgono il loro figlio. L'autorizzazione viene sottoscritta all'iscrizione, o annualmente all'inizio delle attività didattiche;
- non vengono identificati gli alunni all'interno di materiali fotografici online o distribuiti su supporti offline;
- accettando e sottoscrivendo questa policy, i docenti dell'Istituto si impegnano secondo le clausole dette nell'uso dei dispositivi mobili personali per scattare foto/fare dei video ad alunni.

Si rammenta che le riprese -fotografiche, vocali, video- potranno essere eseguite solo per scopi didattici dichiarati, con il consenso delle parti interessate (obbligatoria liberatoria dei genitori o tutori), e tenendo conto delle recenti indicazioni del Garante della privacy.

Registrazioni o immagini effettuate durante lezioni, uscite didattiche o attività di

presentazione allargate (come feste, eventi culturali ecc.…) possono essere utilizzate per usi esclusivamente didattici, di divulgazione delle attività dell'Istituto Comprensivo e di documentazione pedagogica.

La diffusione di contenuti è permessa solo sui canali ufficiali di proprietà dell'Istituto Comprensivo, in ogni caso è sempre subordinata all'autorizzazione del Dirigente Scolastico.

Si richiama l'attenzione di docenti, educatori, esperti sulle possibili conseguenze di eventuali riprese audio/video o fotografiche effettuate all'interno degli ambienti scolastici e successivamente diffuse con l'intento diversi da quelli dichiarati sopra o che ledono la riservatezza e la dignità delle persone può far incorrere in sanzioni disciplinari e pecuniarie o in veri e propri reati.

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.

Per garantire che la rete e i servizi on line d'Istituto vengano utilizzati in modo sicuro, l'Istituto Comprensivo:

- ha elaborato uno specifico regolamento che deve essere accettato e applicato da parte di tutto il personale scolatico e alunni;
- garantisce che l'accesso alle TIC e alla rete avvenga solo ed esclusivamente in presenza di un docente o di personale qualificato della scuola;
- garantisce l'accesso ai servizi online attraverso username unici e password (registro elettronico). L'utente (docente e studente) si impegna a non cedere a nessuno le proprie credenziali/password;
- chiarisce che nessuno dovrebbe accedere con un nome utente non suo ai servizi e dichiara che gli studenti non devono mai essere in possesso dei dati di login degli insegnanti e del personale;
- chiarisce che è necessario che tutti gli utenti si disconnettano quando hanno terminato il lavoro o sono obbligati a lasciare il computer incustodito;
- ribadisce che si dovrebbe lavorare online attraverso una navigazione in incognito;
- fa divieto di utilizzare sessioni lasciate per errore aperte da utenti precedenti. In tali casi è obbligatorio uscire dalla sessione (logout) ed informare l'utente;
- chiarisce che il personale deve assicurare che qualsiasi computer desktop o portatile dalla scuola in prestito di utilizzo è fruito a supporto della sua funzione professionale;
- mantiene tali attrezzature in buono stato e in sicurezza;
- non consente ad alcuna agenzia esterna di accedere in remoto alla propria rete, salvo che non vi sia una chiara necessità professionale; in questo caso l'accesso sarà limitato nel tempo e garantito attraverso sistemi approvati;
- utilizza sistemi di disaster recovery che comprendono uno spazio remoto backup;
- garantisce l'utilizzo del trasferimento e mantenimento sicuro dei dati (pec o in modalità crittografata);
- assicura che tutti i dati sensibili degli allievi o del personale inviati via internet vengano crittografati o inviati e archiviati con sistema sicuro (pec o in modalità crittografata);

Preso atto della criticità della password personale di accesso ai servizi online, l'Istituto

Comprensivo chiarisce che:

- il personale e gli alunni devono sempre mantenere la propria password privata, non deve essere condivisa con gli altri;
- se una password risulta compromessa o dimenticata si deve notificare subito agli uffici di segreteria, che provvederanno ad una sua sostituzione;
- tutto il personale e gli alunni hanno il proprio nome utente e password univoci privati per accedere ai sistemi scolastici (registro elettronico, segreteria digitale, ecc);
- tutti gli utenti (docenti e studenti) hanno la responsabilità di mantenere la(e) propria password(s) privata(e);
- la password personale deve garantire uno standard minimo di sicurezza: pertanto è obbligatorio formarla con almeno 8 caratteri alfanumerici, con maiuscole e minuscole;
- sarebbe auspicabile cambiare le proprie password di accesso almeno 4 volte all'anno (ogni 3 mesi). È obbligatorio in caso di intrusione sospetta ai dati personali.

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.

L'utilizzo degli strumenti di comunicazione online è normato da uno specifico regolamento interno dell'Istituto che ha valore vincolante.

Il sito web istituzionale è gestito da un docente referente con incarico effettivo. I genitori, all'atto dell'iscrizione, esprimono o meno il proprio consenso all'utilizzo di foto e notizie relative agli alunni per l'aggiornamento del sito.

Quando viene pubblicato o linkato il lavoro di altri, il docente referente indica chiaramente gli accrediti alle fonti utilizzate e l'identità o lo stato dell'autore. L'Istituto Comprensivo garantisce che le fotografie pubblicate sul web non verranno mai nominate con nomi completi dei soggetti né avranno didascalie così composte. Non verranno indicati i nomi degli alunni quando verranno salvati file, immagini o tag nella pubblicazione sugli spazi web della scuola.

Il caricamento di informazioni su registro elettronico/segreteria digitale è condiviso tra i diversi membri del personale scolastico e di segreteria in base alle loro competenze: ad esempio tutti gli insegnanti di classe possono caricare informazioni nelle loro aree di pertinenza. Per queste procedure si utilizza il protocollo di navigazione https.

Fotografie e video aventi per soggetto alunni, famiglie e personale scolastico, potranno essere pubblicati solo ed esclusivamente sul sito web istituzionale dal docente referente.

La Didattica Digitale Integrata si serve della piattaforma Google Workspace accreditata presso il Ministero dell'Istruzione. Ogni alunno e il personale scolastico accede con credenziali personali e riservate. La piattaforma è lo strumento di lavoro ufficiale definito tale nel Regolamento di Istitito e nel Patto Educativo di Corresponsabilità pertanto sottoposto alle stesse norme d'uso prevsite per il Registro elettronico. L'attività svolta dagli utenti registrati è monitorata al fine di assicurare la necessaria sicurezza.

3.4 - Strumentazione personale

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

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

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

Il personale scolastico, gli esperti di progetto, gli educatori, i volontari, gli alunni e i genitori o i visitatori che portano all'interno dei plessi scolastici dell'Istituto i dispositivi mobili di loro proprietà ne sono direttamente responsabili: la scuola non risponde direttamente/indirettamente di guasti, smarrimenti, perdita di dati, malfunzionamenti. Va ricordato che i dispositivi mobili personali non possono essere

utilizzati in alcune aree interne o di pertinenza dell'Istituto.

Nell'esercizio delle funzioni di sorveglianza e tutela, il Dirigente Scolastico ha la possibilità di richiedere la verifica ispettiva dei dispositivi personali in caso di ragionevole sospetto che possano contenere materiale illegale o indesiderabile (es. pornografia, violenza o bullismo, registrazioni di qualsiasi genere vietate, ecc.…). L'ispezione verrà eseguita secondo le norme vigenti dagli organi di polizia preposti.

L'Istituto Comprensivo consiglia vivamente a tutti gli studenti di non portare telefoni cellulari e dispositivi mobili personali a scuola. Qualora l'alunno decida di portare con sé il telefono o altro dispositivo mobile, lo fa sotto la sua diretta responsabilità. La scuola non può essere considerata responsabile per manomissioni, furti, danneggiamenti. Sarà cura dell'alunno conservare in un luogo sicuro il dispositivo.

L'uso dei dispositivi personali (telefono, tablet, ecc) è assolutamente vietato in ogni ambiente interno ed esterno di pertinenza della scuola e in ogni contesto didattico/educativo (lezioni, intervalli, pausa mensa, uscite didattiche, ecc). Il dispositivo deve essere tassativamente tenuto spento durante le attività didattiche, educative e ricreative che si svolgono sotto la supervisione e il controllo del personale scolastico (docente, ATA, educatori, ecc).

L'estensione del divieto ai momenti di permanenza a scuola come l'intervallo, la pausa mensa, il cambio dell'ora, ecc., oltre a rispondere a necessità organizzative e di controllo, ha una motivazione educativa. L'Istituto Comprensivo ritiene importante valorizzare momenti di relazione positiva tra gli studenti, evitando atteggiamenti di esclusione, di isolamento e di separazione dalla vita scolastica reale.

In caso di necessità ed emergenze, sarò cura del personale scolastico contattare le famiglie per conto dell'alunno, o, viceversa, lo studente per conto dei famigliari, attraverso i canali ufficiali della scuola (telefono del plesso scolastico, mail istituzionale).

Se un alunno viola questa Policy, il dispositivo verrà immediatamente confiscato dal personale in servizio, il quale lo deporrà in un luogo sicuro in ufficio di segreteria. Contestualmente verrà data comunicazione ai genitori in forma scritta/orale attraverso i canali ufficiali scuola-famiglia (telefono, diario, registro elettronico).

La restituzione dei dispositivi sequestrati verrà effettuata secondo le modalità previste dal Regolamento di Istituto, comunque durante un incontro tra docente e famiglia in cui, se necessario, verrà notificata l'eventuale sanzione disciplinare.

Telefoni e dispositivi personali non possono essere mai usati durante gli esami o le prove nazionali.

Il personale che svolge la propria mansione all'interno degli ambienti scolastici (docenti, ATA, educatori, volontari, specialisti, ecc) non è autorizzato a utilizzare i propri telefoni cellulari o dispositivi a titolo professionale, come ad esempio per

contattare i bambini, i ragazzi e le loro famiglie all'interno o al di fuori del proprio orario di lavoro e dall'Istituto.

Tutti i visitatori sono invitati a mantenere i loro telefoni e dispositivi personali su silenzioso.

Per ragioni di privacy e sicurezza, la comunicazione Bluetooth dovrebbe essere impostata in modalità nascosta o spenta.

Il personale scolastico (docenti, ATA, educatori, volontari, ecc) in servizio è tenuto a mantenere i propri dispositivi spenti, fatta eccezione se utilizzati per lo svolgimento dell'attività didattica (es. completamento del registro elettronico).

In ogni caso il personale in servizio deve evitare di essere raggiunto da qualsiasi notifica o segnalazione o eventi particolarmente distraenti e disturbanti la stessa attività didattica.

I cellulari non dovranno essere utilizzati durante l'insegnamento e/o l'attività didattica ed educativa, a meno che non sia stato concesso un permesso esplicito dal Dirigente Scolastico.

Il divieto si applica anche negli intervalli e in altre situazioni che sono assimilabili ad attività didattica/educativa come mensa, cambio dell'ora, intervalli.

In linea di principio, il personale scolastico (docenti, ATA, educatori, volontari, ecc) non deve utilizzare dispositivi di proprietà personale, come cellulari o macchine fotografiche, per scattare foto, video, registrazioni audio/video che coinvolgano gli alunni, e preferenzialmente utilizzare solo le attrezzature adatte allo scopo di proprietà della scuola.

Se la scuola non possedesse tali attrezzature, potrà utilizzare le proprie previo permesso del Dirigente Scolastico, e seguire le norme illustrare nel presente documento.

In caso di necessità si può fare uso di abbonamenti personali.

In caso di emergenza, il docente o qualsiasi altro membro del personale della scuola (compresi educatori ed esperti di progetto), se non ha accesso immediato e semplice a un dispositivo di proprietà della scuola, è autorizzato ad utilizzare il proprio cellulare stando attento a non divulgare dati sensibili o personali. Dovrà comunque riferire l'incidente al Dirigente Scolastico.

Il personale della scuola ha facoltà di utilizzo del proprio telefono cellulare durante i periodi di pausa, seguendo le regole generali di non disturbo delle attività.

Le infrazioni a queste norme, possono comportare il richiamo formale da parte del Dirigente Scolastico, e altre sanzioni ritenute necessarie in funzione alla gravità della situazione.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco di una annualità).

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

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

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

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

Nell'ambito della sensibilizzazione alle tematiche prese in esame in questo capitolo e della definizione di un perimetro di prevenzione, l'Istituto Comprensivo di Rivarolo è già orientato ed attivo nell'informare i vari settori di utenza delle specificità di ciascuna di queste attraverso documenti liberamente scaricabili dal proprio sito web e attraverso iniziative con specialisti. Documenti e inziative, oltre all'obiettivo di

formare/informare gli utenti, intendono spingere le persone a desiderare un cambiamento, pongono in evidenza la possibilità di generare un cambiamento e cercano di individuare le azioni che consentono di produrre il cambiamento.

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).

Per al segnalazione di casi di bullismo e cyberbullismo si rimanda al capitolo successivo.

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.

Per al segnalazione di casi di hate speech si rimanda al capitolo successivo.

4.4 - Dipendenza da Internet e gioco online

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

scolastico e irrefrenabile voglia di utilizzo della Rete.

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

L'Istituto Comprensivo, nell'ambito dell'educazione al benessere psico-fisico, promuove costantemente l'adozione di un comportamento adeguato circa l'uso consapevole di Internet e dei videogiochi (non solo online). In collaborazione con il responsabile di Istitiuto per la prevenzione delle dipendenze, si sta valutando un percorso educativo strutturato e interdisciplinare più articolato ed efficace.

Già ora la scuola disponde di risorse professionali adegaute (es. sportello psicologico interno) a cui ricorre quando necessario per trarre il necessario supporto.

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.

Per al segnalazione di casi di sexting si rimanda al capitolo successivo.

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.

Poichè la problematica dell'adescamento online si inquadra in uno scenario più ampio di scarsa educazione emotiva, sessuale e di assenza di competenza digitale, l'Istituto Comprensivo ha già avviato percorso di educazione digitale e di benessere curricolare (integrato nella programmazione di veri discipline come Tecnologia, Educazione Civica, Lettere, Religione ecc) in cui viene evidenziato il valore della privacy e della gestione dell'immagine e dell'identità online, e si sostiene il percorso di maturazione degli alunni nella capacità di gestire adeguatamente le proprie relazioni online.

Per al segnalazione di casi di adescamento online si rimanda al capitolo successivo.

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.

Per al segnalazione di casi di pedopornografia si rimanda al capitolo successivo.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco di una annualità).

- Promuovere incontri/iniziative di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Promuovere incontri/iniziative informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.
- Promuovere incontri/iniziative per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Promuovere incontri/iniziative di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo

svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

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

- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

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

segnalare la presenza di materiale pedopornografico online.

I segnali sociali che possono insospettire il personale scolastico (docente, ATA, educatore, ecc) vanno dal chiacchierio prolungato in classe dopo i momenti ricreativi, ai cambiamenti improvvisi nel modo di porsi con i pari. Dal calo nel rendimento scolastico apparentemente immotivato all'isolamento volontario dal gruppo. Offriamo qui un elenco indicativo e non esaustivo dei possibili elementi da segnalare:

- l'alunno appare nervosa quando riceve un messaggio o una notifica;
- l'alunno sembra a disagio nell'andare a scuola o finge di essere malata;
- l'alunno cambia comportamento ed atteggiamento in modo repentino;
- l'alunno mostra ritrosia nel dare informazioni su ciò che fa online;
- l'alunno soprattutto dopo essere stato online, mostra rabbia o si sente depresso;
- l'alunno inizia ad utilizzare sempre meno Pc e telefono (arrivando ad evitarli);
- l'alunno perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;
- l'alunno può evidenziare un ritiro sociale;
- l'alunno ha conoscenze sessuali non adeguate alla sua età;
- l'alunno si isola totalmente e sembra preso solo da una relazione online;

Va ricordato che il docente, l'educatore, e più in generale il personale in servizio presso una scuola deve farsi guidare dal principio del "superiore interesse del minore". La priorità non è trovare il responsabile. Nell'immediato occorre evitare indagini e limitarsi e registrare quanto accaduto.

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.

Tutto il personale scolastico (docente, ATA, educatori, psicologo) è chiamato a raccogliere le richieste/segnalazioni degli alunni e a segnalare ogni anomalia legata ad atti e comportamenti illegali, inopportuni e violenti. Il Coordinatore di Classe, "collettore primario" delle segnalazioni, è un elemento fondamentale di raccordo tra il Consiglio di Classe, che deve essere messo a conoscenza dei fatti nei tempi e luoghi opportuni, e il Responsabile di Istituto e il Dirigente Scolastico.

Se in prima battuta la comunicazione verbale immediata tra Coordinatore di Classe e Responsabile di Istituto e Dirigente Scoalstico è necessaria per applicare i necessari interventi di contenimento della situazione, è altresì necessario la compilazione dell'apposito modulo digitale per la segnalazioni di casi presente sul sito web di Istituto affinchè la procedura di tracciamento, analisi e gestione dell'evento avvenga tenendo conto di tutte le circostanze e le procedure interne.

Ogni alunno è tenuto, per rispetto e solidarietà nei confronti degli altri studenti, ha segnalare verbalmente ai docenti o attraverso il modulo digitale presente sul sito web di Istituto, fatti accaduti o anche solo sospetti circa le difficoltà mostrate dai propri compagni. Diversamente, se l'alunno è vittima di violenza, ingiurie o prevaricazioni,

può in qualunque momento riferirsi al docente di classe che avvierà l'iter di gestione della richiesta.

Qualora sia la famiglia di un alunno a fare la segnalazione, questa potrà rivolgersi al docente di classe o inviare il modulo digitale presente sul sito web della scuola.

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

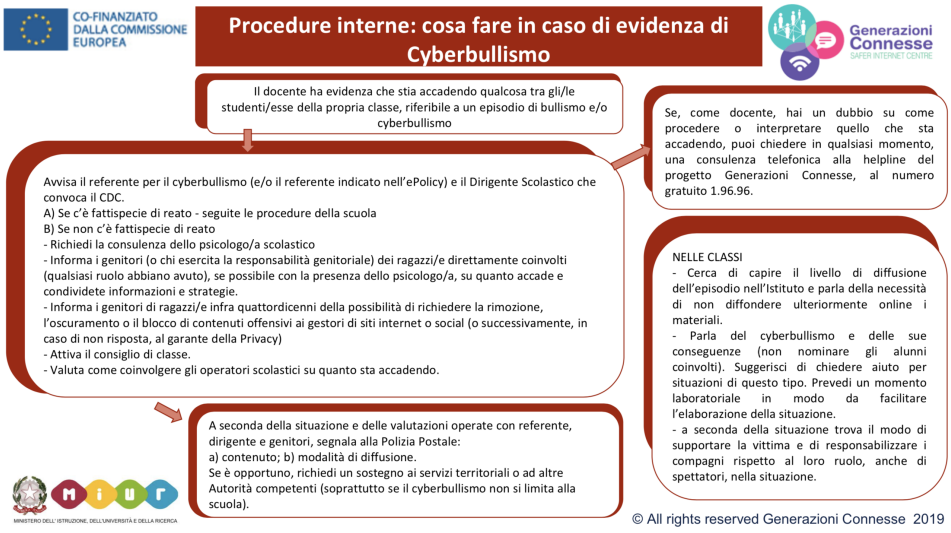
segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.

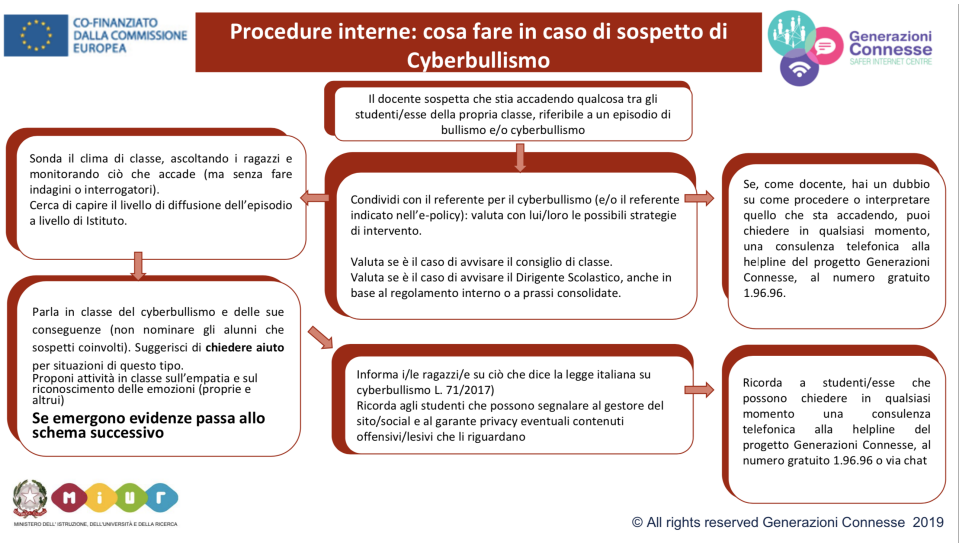
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

L'Istituto Comprensivo di Rivarolo Canavese, al fine di gestire le segnalazioni e dare il necessario supporto agli alunni interessati, lavora a stretto contatto con le Forze di Polizia, con gli organi competenti e con gli enti/associazioni territoriali.

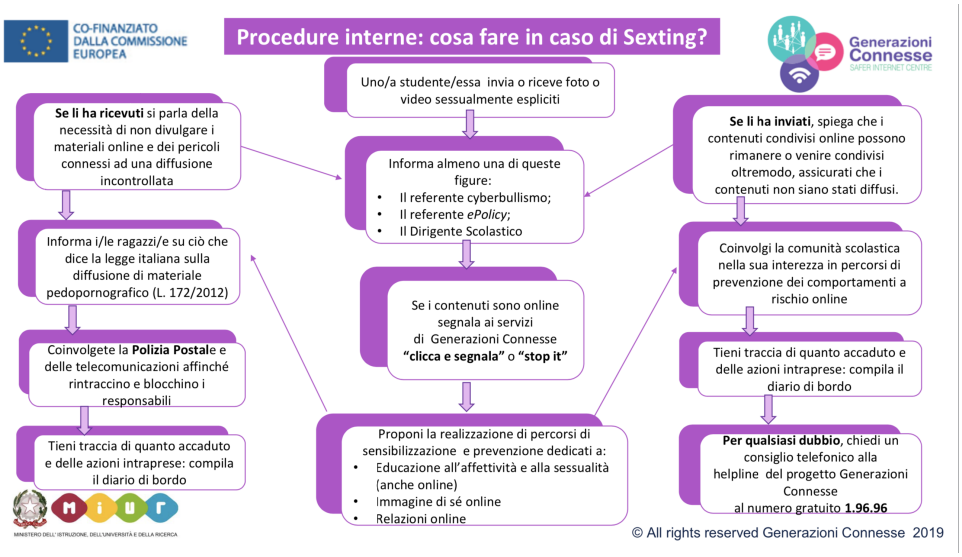
5.4. - Allegati con le procedure

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

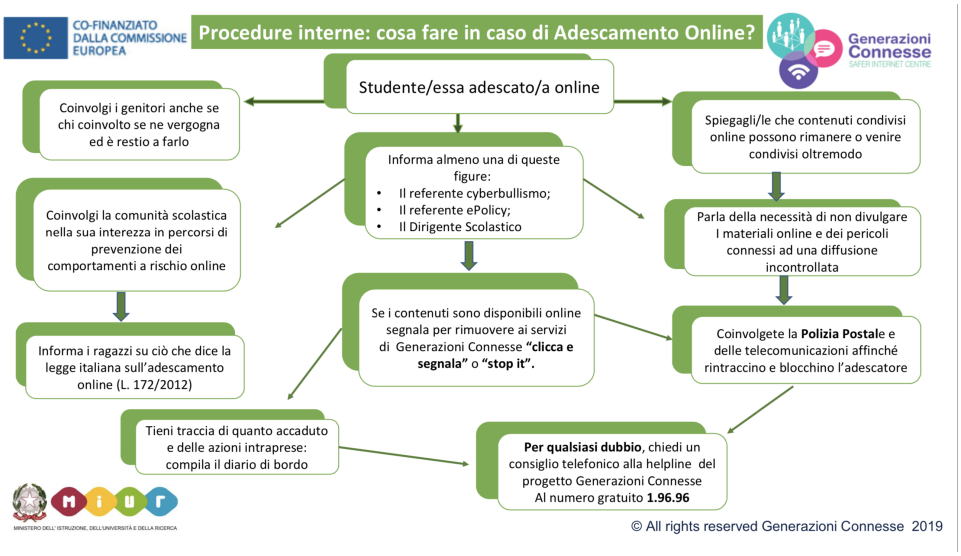




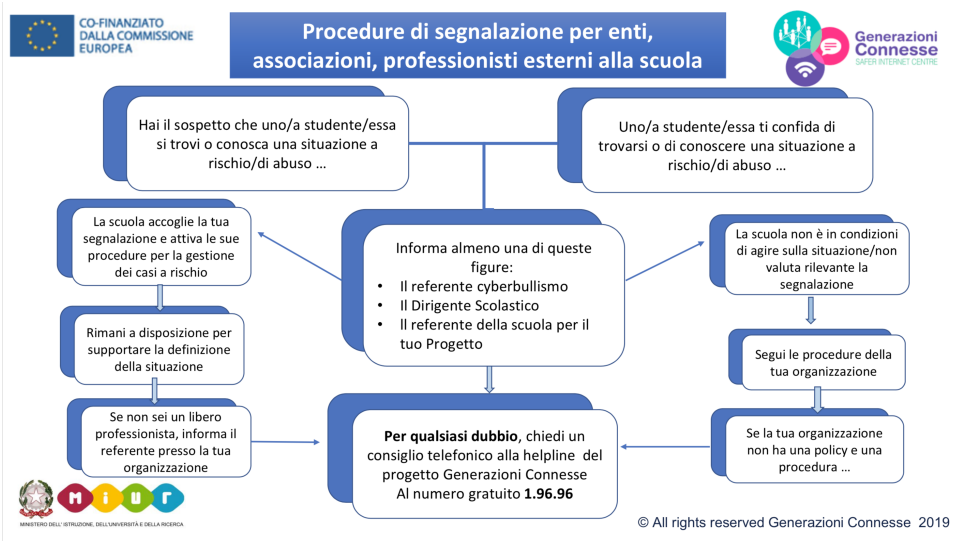
Procedure interne: cosa fare in caso di sexting?



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

Gestione dei casi di "lieve entità"

Rischio	Azioni	Tempi di esecuzione
Accesso a contenuti inopportuni di qualsiasi genere attraverso motori di ricerca via Internet e postazioni fisse di proprietà dell'Istituto	Filtraggio selettivo mediante apparecchiature hardware	In base alla disponibilità economica
Accesso a contenuti inopportuni di qualsiasi genere attraverso accesso al WiFi dell'Istituto con mobile device di Istituto o device personali autorizzati	Filtraggio selettivo mediante apparecchiature hardware.	In base alla disponibilità economica
Smarrimento password personale o di sospetto furto d'identità per servizi on line di Istituto	Formazione continua al mantenimento in sicurezza del proprio account;	Durante le attività didattiche curricolari/extracurricolari
	Immediata informazione degli uffici di segreteria	Contestuale alla rilevazione del problema
	Blocco utenza. Reset o cancellazione/rinnovo dell'utenza interessata	Entro 24 ore dalla segnalazione/in base ai tempi tecnici della piattaforma in uso
Uso non positivo e non adeguato delle TIC intese nel più largo senso possibile	Formazione continua attraverso laboratori o conferenze rivolti a tutte le componenti della comunità scolastica	Durante l'anno scolastico
	Monitoraggio di comportamenti suscettibili di attenzione secondo le indicazioni date da "Generazioni connesse".	Contestualmente agli eventi, il Referente di Istituto per il bullismo e il cyberbullismo mantiene attivo un registro delle segnalazioni in cui si annotano i casi e le contromisure attivate (vedi allegato alla Policy). Il DS valuta celermente eventuali denunce agli organi governativi di competenza.
	Condivisione tra tutti i membri della comunità scolastica interessati. Eventuale denuncia alle autorità governative di competenza. Segnalazione alla psicopedagogista, responsabile dello sportello di ascolto della Scuola per consulto e accompagnamento nelle azioni.	Celermente, in base alla disponibilità del Consiglio di Classe o Interclasse. In base alla disponibilità delle figure professionali esterne.

Uso non consentito dei dispositivi fissi e mobili di proprietà della scuola o personali	Formazione continua rivolta a tutte le componenti della comunità scolastica. Sequestro immediato dello strumento personale. Attivazione contestuale delle procedure di segnalazione alla famiglia.	La formazione avverrà durante il normale anno scolastico. Gli interventi correttivi e di segnalazione sono contestuali all'evento.

Gestione dei casi di "media entità"

Cosa segnalare	Come segnalare	Come gestire
Navigazione in siti inadeguati. Documenti inadeguati lasciati su pc e/o condivisi. Acquisizione e/o uso di immagini, registrazioni video e audio, documenti in modo non congruo alla policy	**In caso di minore:** registrazione sul registro di classe con comunicazione alla famiglia **Per tutti:** Immediata comunicazione orale: al Referente di Istituto e contestualmente al Dirigente Scolastico/Vicario e Fiduciario di plesso. Compilazione della scheda di segnalazione da inoltrare alla segreteria (vedi allegato) Nei casi di particolare gravità è richiesta la verbalizzazione da parte del personale interessato da allegare al registro del Referente d'Istituto	Ogni segnalazione verrà valutata dal DS e dal Referente d'Istituto per il bullismo e il cyberbullismo che attiveranno celermente, a seconda della gravità dei fatti e rispetto alle evidenze, le procedure di sanzione (compreso quelle di competenza degli organi collegiali) e se necessario gli enti governativi competenti con relativo verbale di accompagnamento.

Discussioni via mail, social o chat istantanee che influiscono in modo negativo sui comportamenti assunti o usate in modo difforme dalla Policy (anche casi di abusi, cyberbullismo, bullismo ecc..)	**Per tutti:** Immediata comunicazione orale al Referente di Istituto e contestualmente al Dirigente Scolastico/Vicario e Fiduciario del plesso. In ogni caso il D.S. deve essere messo tempestivamente al corrente. Compilazione della scheda di segnalazione da inoltrare alla segreteria (vedi allegato) In caso di situazione particolarmente grave, verrà richiesta contestualmente una verbalizzazione scritta da parte del dichiarante e, se si tratta di minore, ci sarà il coinvolgimento immediato dei genitori.	Ogni segnalazione verrà valutata dal DS e dal Referente d'Istituto che attiveranno celermente, a seconda della gravità dei fatti e rispetto alle evidenze, le procedure di sanzione/accompagnamento (comprese quelle di competenza degli organi collegiali) e se necessario gli enti governativi competenti con relativo verbale di accompagnamento.

Il nostro piano d'azioni

Non è prevista nessuna azione.