Documento di ePolicy

GRIC827009

IC FOLLONICA 1

VIA GORIZIA 11 - 58022 - FOLLONICA - GROSSETO (GR)

elisa ciaffone

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

1. **Presentazione dell'ePolicy**
    1. Scopo dell'ePolicy
    2. Ruoli e responsabilità
    3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
    4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
    5. Gestione delle infrazioni alla ePolicy
    6. Integrazione dell'ePolicy con regolamenti esistenti
    7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
2. **Formazione e curricolo**
    1. Curricolo sulle competenze digitali per gli studenti
    2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
    3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
    4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
    1. Protezione dei dati personali
    2. Accesso ad Internet
    3. Strumenti di comunicazione online
    4. Strumentazione personale
4. **Rischi on line: conoscere, prevenire e rilevare**
    1. Sensibilizzazione e prevenzione
    2. Cyberbullismo: che cos'è e come prevenirlo
    3. Hate speech: che cos'è e come prevenirlo
    4. Dipendenza da Internet e gioco online
    5. Sexting
    6. Adescamento online
    7. Pedopornografia
5. **Segnalazione e gestione dei casi**
    1. Cosa segnalare
    2. Come segnalare: quali strumenti e a chi
    3. Gli attori sul territorio per intervenire
    4. Allegati con le procedure

Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

Il presente Documento è parte integrante del PTOF e le azioni sottoscritte costituiscono indicazioni e buone prassi di azione e prevenzione in materia di bullismo e cyberbullismo.

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.

Nell'ambito di questa e-Policy sono individuati i seguenti ruoli e le principali responsabilità correlate:

IL DIRIGENTE SCOLASTICO

- è garante della sicurezza, anche online, di tutti i membri della comunità scolastica;
- promuove la cultura della sicurezza online attivando, con la collaborazione del Referente di Istituto per il bullismo /cyberbullismo, percorsi di formazione per la sicurezza e le problematiche connesse all'utilizzo della RETE sia online che offline;
- garantisce l'esistenza di un sistema/protocollo per il monitoraggio e il controllo interno della sicurezza online;
- gestisce e interviene nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali da parte degli studenti e delle studentesse.

L'ANIMATORE DIGITALE

- supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali;
- promuove percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale";
- monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a

scuola.

IL REFERENTE BULLISMO E CYBERBULLISMO

- coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e cyberbullismo, avvalendosi anche delle Forze di Polizia, delle associazioni e degli enti territoriali.

I DOCENTI

- integrano parti del curricolo disciplinare con approfondimenti sull'uso responsabile delle TIC e della RETE, servendosi delle tecnologie digitali nella didattica (LIM o altri dispositivi tecnologici);
- sviluppano le competenze digitali degli allievi facendo sì che gli stessi conoscano e seguano le norme di sicurezza nell'utilizzo del web sia per attività in presenza sia per attività didattiche extracurricolari;
- comunicano prontamente alle famiglie eventuali problematiche emerse in classe nell'utilizzo del digitale e stabiliscono linee comuni di intervento educativo;
- segnalano al Dirigente scolastico e ai suoi collaboratori qualunque violazione, anche online, del Regolamento di Istituto secondo la procedura stabilita.

IL PERSONALE ATA

- svolge funzioni di tipo amministrativo, contabile, gestionale e di sorveglianza, connesse alle attività dell'Istituzione scolastica, in collaborazione con il Dirigente scolastico e con il personale docente;
- favorisce l'accesso alla Rete della scuola agli utenti autorizzati con apposita password, per scopi istituzionali e consentiti;
- collabora nel reperire, verificare e valutare informazioni inerenti possibili casi di bullismo/cyberbullismo.

STUDENTI E STUDENTESSE

- in relazione al proprio grado di maturità e di consapevolezza raggiunta e in coerenza con quanto richiesto dai docenti, devono rispettare le norme che disciplinano l'uso corretto e responsabile delle tecnologie digitali, come indicato nel Regolamento di Istituto;
- con il supporto della scuola devono imparare a tutelarsi online e adottare le regole di e-safety per evitare situazioni di rischio per sé e per gli altri;
- devono partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education.

I GENITORI

- partecipano alle iniziative di sensibilizzazione e formazione organizzate dall'Istituto sull'uso consapevole delle TIC e della RETE, nonché sull'uso

responsabile dei device personali;
- condividono con i docenti le linee educative relative alle TIC e alla RETE, al Regolamento di Istituto, al patto di corresponsabilità educativa e al documento di e-Policy dell'Istituto;
- collaborano con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite.

GLI ENTI EDUCATIVI ESTERNI E LE ASSOCIAZIONI

- osservano le politiche interne sull'uso consapevole della Rete e delle TIC;
- attivano procedure e comportamenti sicuri per la protezione degli studenti e delle studentesse durante le attività che vengono svolte all'interno della scuola o in cui sono impegnati gli stessi.

Per quanto non espressamente indicato sui ruoli e sulle responsabilità delle figure presenti all'interno dell'Istituzione scolastica, si rimanda:

all'art. 21, comma 8, Legge 15 marzo 1997, n. 59; all'art. 25 della Legge 30 marzo 2001, n. 165; al CCNL in vigore; al D.P.R. 8 marzo 1999, n. 275; alla Legge 13 luglio 2015, n. 107; al Piano Nazionale Scuola Digitale; a quanto stabilito in materia di culpa in vigilando, culpa in organizzando, culpa in educando (art. 2048 c.1-2 c.c.).

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).

Ambiti di applicazione, attività e ruoli.

Le attività di progettazione o di formazione devono essere preventivamente autorizzate dal Dirigente Scolastico, con modalità e tempi concordati. A tal proposito i soggetti esterni dovranno fornire un programma delle attività stesse al fine di essere autorizzato dalla Dirigenza.

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.

Condivisione del documento di e-Policy alla Comunità scolastica ed ai genitori degli studenti e delle studentesse.

Le norme adottate e sottoscritte dalla scuola in materia di sicurezza ed utilizzo delle tecnologie digitali, saranno rese note tramite pubblicazione del presente documento sul sito web della scuola.

Condivisione e comunicazione dell'e-Policy agli studenti e alle studentesse.

- agli alunni da parte dei docenti, verrà presentata la e-Policy insieme ai regolamenti correlati e al Patto di corresponsabilità;
- tutti gli alunni saranno informati che la rete, l'uso di internet e di ogni dispositivo digitale saranno controllati dai docenti e utilizzati solo con la loro autorizzazione e supervisione;
- 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, con specifico riferimento al contrasto di ogni forma di cyberbullismo.

Condivisione e comunicazione dell'e-Policy al personale scolastico.

- le norme adottate dalla scuola in materia di sicurezza dell'uso del digitale saranno discusse dagli organi collegiali e rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito istituzionale;
- il personale scolastico riceverà un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso materiali resi disponibili anche sul sito istituzionale, nonché mediante la partecipazione a incontri formativi organizzati dall'Istituto;
- tutto il personale deve essere consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

Condivisione e comunicazione dell'e-Policy ai genitori.

- sarà favorito un approccio collaborativo nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione di incontri scuola- famiglia assembleari, collegiali e individuali;
- al fine di sensibilizzare le famiglie sui temi dell'uso delle TIC saranno organizzati incontri informativi per presentare e condividere la presente e-Policy.

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.

DISCIPLINA DEGLI ALUNNI

Le potenziali infrazioni in cui potrebbero incorrere gli alunni, relativamente alla fascia di età considerata, nell'utilizzo delle tecnologie digitali e di internet durante la

didattica sono le seguenti:

- uso della RETE per giudicare, infastidire, offendere, denigrare, impedire a qualcuno di esprimersi o partecipare, esprimersi in modo volgare usando il turpiloquio;
- invio incauto o senza permesso di foto o altri dati personali (indirizzo di casa, numero di telefono)
- condivisione online di immagini o video di compagni/e e del personale scolastico senza il loro esplicito consenso o che li ritraggono in pose offensive e denigratorie;
- condivisione di immagini intime e a sfondo sessuale;
- invio di immagini o video volti all'esclusione di compagni/e; comunicazione incauta e senza permesso con sconosciuti; collegamenti a siti web non adeguati e non indicati dai docenti.

L'azione educativa prevista per gli alunni è rapportata alla fascia di età e al livello di sviluppo e maturazione personale. Pertanto sono previsti interventi graduali in base all'età e alla gravità delle violazioni e da attivare previa audizione dell'alunno:

- richiamo verbale;
- richiamo scritto con annotazione sul diario e sul registro;
- convocazione dei genitori da parte dell'insegnante;
- convocazione dei genitori da parte del Dirigente Scolastico.

Contestualmente sono previsti interventi educativi di rinforzo rispetto a comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza, di prevenzione e gestione positiva dei conflitti, di pro-socialità, di conoscenza e gestione delle emozioni.

E', inoltre, importante intervenire su tutto il contesto classe con attività specifiche educative e di sensibilizzazione.

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 allievi:

- utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di docenza o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiale non idoneo;
- utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- trattamento dei dati personali e dei dati sensibili degli alunni non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- diffusione delle password assegnate e una custodia non adeguata degli

strumenti e degli accessi di cui possono approfittare terzi;
- carente istruzione preventiva degli alunni sull'uso corretto e responsabile delle TIC e di internet;
- mancata vigilanza sugli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili rischi connessi a 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 disporre il controllo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola; può disporre la cancellazione di materiali non adeguati o non autorizzati dal sistema informatico della scuola, e se necessario ne conserva una copia per eventuali approfondimenti successivi.

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 dei procedimenti che possono avere carattere organizzativo-gestionale, disciplinare, amministrativo, penale, a seconda del tipo e della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

DISCIPLINA DEI GENITORI

In considerazione dell'età degli studenti e delle studentesse e della loro dipendenza dagli adulti, anche talune condizioni e condotte dei genitori medesimi possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli allievi a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico. Gli atteggiamenti da parte della famiglia più opportuni sono:

- predisporre una postazione del computer visibile e controllabile dall'adulto;
- controllo del proprio figlio nella navigazione sul web e nell'uso di cellulare, smartphone o tablet;
- evitare un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali, indirizzi di siti o contenuti non idonei a minori.

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 sè e/o dannosi per altri (culpa in educando e in vigilando).

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

La e-Policy è coerente con quanto stabilito nei Regolamenti vigenti e col Patto di Corresponsabilità educativa.

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 e la revisione dell'e-Policy saranno svolti annualmente e/o qualora si verifichino cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno dell'Istituto.

L'aggiornamento del documento di e-Policy sarà curato dal Referente d'Istituto e, ove possibile, con la partecipazione dell'Animatore Digitale.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.

Azioni da svolgere nei prossimi 3 anni:

- Organizzare 1 evento di presentazione 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.

La competenza digitale, per la sua importanza nelle attività quotidiane e professionali, è ritenuta dall'Unione Europa una competenza chiave per lo sviluppo della cittadinanza (Raccomandazione del Consiglio Europeo relativa alle competenze chiave per l'apprendimento permanente, 2018). Nel curricolo verticale di Educazione Civica del nostro Istituto, sulla base di quanto disposto dall'art. 5 della legge 20 agosto 2019 n. 92 (Introduzione dell'insegnamento scolastico dell'educazione civica) interamente dedicato alla "cittadinanza digitale", tale competenza pervade in modo trasversale tutti gli insegnamenti, con la finalità di fornire agli alunni, alla fine del primo ciclo d'istruzione, tutti gli strumenti necessari per un approccio consapevole, critico, autonomo e responsabile alle tecnologie digitali e ai mezzi di comunicazione virtuali. Tali competenze sono oggetto di certificazione, come da apposito documento ministeriale, al termine della Scuola Primaria e Secondaria. Negli ultimi anni l'Istituto ha provveduto all'implementazione della donazione digitale nei vari Plessi, anche attraverso la partecipazione a progetti PON, per consentire l'introduzione di

metodologie basate dell'uso delle TIC.

Le Indicazioni Nazionali (2012 e aggiornamento del 2018 alla luce del quadro normativo europeo, in accordo con la già citata Raccomandazione) prevedono che al termine del primo ciclo d'istruzione lo studente possegga buone competenze digitali e sappia usare con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di apprendimento, di controllo e di verifica per interagire con soggetti diversi nel mondo. In questo senso le TIC preparano gli studenti ad un'attiva e consapevole partecipazione ad una società in rapida evoluzione e nella quale è necessario acquisire abilità e competenze in grado di facilitare l'adattamento dell'individuo a continui cambiamenti.

Le finalità formative delle TIC (PNSD, Spazi e ambienti per l'apprendimento) possono essere sintetizzate nei seguenti punti:

- favorire la conoscenza dello strumento pc e/o tablet a scopo didattico;
- sostenere l'alfabetizzazione informatica;
- favorire la trasversalità delle discipline;
- facilitare il processo di apprendimento;
- favorire il processo di inclusione;
- fornire nuovi strumenti a supporto dell'attività didattica;
- promuovere situazioni collaborative di lavoro e di studio;
- sviluppare creatività e capacità di lavorare in gruppo;
- promuovere azioni di cittadinanza attiva;
- utilizzare in modo critico, consapevole e collaborativo la tecnologia.

TRAGUARDI PER LO SVILUPPO DELLE COMPETENZE

Al termine della Scuola dell'Infanzia

- Esplora e sperimenta le prime forme di comunicazione, incontrando anche le

tecnologie digitali e i nuovi media.

- Si interessa a macchine e strumenti tecnologici, sa scoprirne le funzioni e i possibili usi.

Al termine della Scuola Primaria

- Produce semplici modelli o rappresentazioni grafiche del proprio operato utilizzando elementi del disegno tecnico o strumenti multimediali.

- Inizia a riconoscere in modo critico le caratteristiche, le funzioni e i limiti della tecnologia attuale.

TRAGUARDI PER LO SVILUPPO DELLE COMPETENZE

AL termine della Scuola Secondaria di I grado

- Conosce le proprietà e le caratteristiche dei diversi mezzi di comunicazione ed è in grado di farne un uso efficace e responsabile rispetto alle proprie necessità di studio e socializzazione.

- Sa utilizzare comunicazioni procedurali e istruzioni tecniche per eseguire, in maniera metodica e razionale, compiti operativi complessi, anche collaborando e cooperando con i compagni.

- Progetta e realizzare rappresentazioni grafiche o infografiche, relative alla struttura e al funzionamento di sistemi materiali o immateriali, utilizzando elementi del disegno tecnico o altri linguaggi multimediali e di programmazione.

Le Competenze digitali declinate tengono conto delle cinque aree del quadro di riferimento DigComp 2.1 (Quadro comune di riferimento europeo per le competenze digitali) elaborato dalla Commissione Europea nel 2021.

INFORMAZIONE: identificare, localizzare, recuperare, conservare, organizzare e analizzare le informazioni digitali, giudicare la loro importanza e lo scopo;

COMUNICAZIONE: comunicare in ambienti digitali, condividere risorse attraverso strumenti on-line, collegarsi con gli altri e collaborare attraverso strumenti digitali, interagire e partecipare alle comunità e alle reti;

CREAZIONE DI CONTENUTI: creare e modificare nuovi contenuti (da elaborazione testi a immagini e video); integrare e rielaborare le conoscenze ed i contenuti;

produrre espressioni creative, contenuti media e programmare; conoscere e applicare i diritti di proprietà intellettuale e le licenze;

SICUREZZA: protezione personale, protezione dei dati, protezione dell'identità digitale, misure di sicurezza, uso sicuro e sostenibile;

PROBLEM-SOLVING: identificare i bisogni e le risorse digitali, valutare appropriati strumenti digitali secondo lo scopo o necessità, risolvere problemi concettuali attraverso i mezzi digitali, utilizzare creativamente le tecnologie, risolvere problemi tecnici, aggiornare la propria competenza e quella altrui.

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.

La competenza digitale oggi è imprescindibile, sia per i docenti, sia per gli alunni, e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa ed in grado di venire incontro ai nuovi stili di apprendimento.

L'attenzione all'uso delle TIC nella didattica, infatti, rende gli apprendimenti più motivanti, coinvolgenti ed inclusivi, con una funzione di guida da parte del docente; inoltre, permette di sviluppare capacità che sono sempre più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza ed il confronto fra pari in modalità sincrona.

Pertanto, il Collegio docenti riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola, sia quelle liberamente scelte dai docenti (anche online) purché restino coerenti con il piano di formazione, come meglio indicato nel PTOF.

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.

Ciò avverrà tramite specifici momenti di formazione formulati secondo un'analisi del fabbisogno del corpo docente sull'utilizzo ed integrazione delle TIC nella didattica o legati all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui gli alunni accedono sempre più autonomamente.

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

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

L'Istituto si impegna alla diffusione delle informazioni e delle procedure contenute nel documento Policy e-safety per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'Istituto e prevenire i rischi legati a

un utilizzo non corretto di Internet.

Inoltre, saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo.

Sul sito scolastico e sulla relativa sezione virtuale relativa a "Generazioni connesse" saranno messi in condivisione materiali dedicati agli alunni e alle famiglie che possono fornire spunti di approfondimento e confronto.

In sintesi:

Gli studenti e le studentesse devono attenersi a quanto previsto dai Regolamenti scolastici e dalle Circolari interne emanate dal Dirigente scolastico, sulla base delle note ministeriali sull'utilizzo consapevole delle tecnologie digitali all'interno del contesto scolastico.

I genitori, nell'azione di corresponsabilità didattico-educativa, rappresentano un punto di forza per l'implementazione dei rapporti "scuola-famiglia", quale garanzia e rispetto degli impegni, di natura anche pedagogica, sottoscritti e condivisi nello stesso Patto di corresponsabilità.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023)

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

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

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

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.

Di seguito viene riportata la modulistica che ha lo scopo di adempiere a quanto previsto dalla normativa vigente in materia di autorizzazione per l'utilizzo di fotografie o video resa dai genitori degli alunni minorenni (D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" e successivi aggiornamenti)".

LIBERATORIA PER L'UTILIZZO DI FOTOGRAFIE O VIDEO

I sottoscritti, Sig._____
[Nome e Cognome dell'soggetto interessato] (1)

e Sig.ra_____, in qualità di
[Nome e Cognome dell'soggetto interessato] (2)

Genitori/Tutori del/la minore_____
[Nome e Cognome dell'soggetto interessato]

con riferimento alle foto e/o alle riprese audio/video scattate e/o riprese dal personale dell'Istituto Comprensivo Follonica 1 (di seguito "**Istituto**") con la presente:

AUTORIZZANO

a titolo gratuito, anche ai sensi degli artt. 10 e 320 cod. civ. e degli artt. 96 e 97 legge 22.4.1941, n. 633, Legge sul diritto d'autore, l'utilizzo delle foto o video ripresi durante le attività scolastiche, le iniziative e gli eventi organizzati dalla scuola durante l'anno scolastico che riprendono nostro/a figlio /figlia, nonché autorizzano la conservazione delle foto e degli audio/video stessi negli archivi informatici dell'**Istituto Comprensivo Follonica 1**.

INFORMATIVA SULLA PRIVACY

Gentile interessato che fornisce all' Istituto Comprensivo Follonica 1 (di seguito "Istituto") i suoi dati personali, desideriamo informarLa che il "Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati" (da ora in poi GDPR) prevede la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. L'**Istituto**, in qualità di "Titolare" del trattamento, ai sensi dell'articolo 13 del GDPR, pertanto, Le fornisce le seguenti informazioni:

Finalità del trattamento:
L'Istituto tratterà i dati personali dello studente per la realizzazione di album ricordo agli allievi – presentazione delle attività durante l'open day - foto e/o cartelloni ad uso interno - riproduzione di video e/o materiale fotografico video a scopi documentaristici, didattici, formativi e informativi - articoli di cronaca di giornali o quotidiani locali relativi ad eventi di cui la scuola è stata parte attiva. Sono esclusi, pertanto, scopi pubblicitari.

Modalità di trattamento dei dati:
I dati personali da Voi forniti formeranno oggetto di operazioni di trattamento nel rispetto della normativa sopracitata e degli obblighi di riservatezza cui è ispirata l'attività dell'Istituto. Tali dati verranno trattati sia con strumenti informatici sia su supporti cartacei sia su ogni altro tipo di supporto idoneo (es. CD, DVD, Pen Drive), nel rispetto delle misure di sicurezza previste dal GDPR.

Obbligatorietà o meno del consenso:
Il conferimento dei Suoi dati è facoltativo. Il mancato consenso non permetterà l'utilizzo delle immagini e/o delle riprese audiovisive del soggetto interessato per le finalità sopra indicate.

Comunicazione e diffusione dei dati:
Nei limiti pertinenti alle finalità di trattamento indicate, i dati personali dello studente (immagini e riprese audiovisive) potranno essere comunicati a genitori di altri studenti in strutture educative, convegni, mostre, eventi, feste. Tali dati saranno oggetto di diffusione sul sito internet istituzionale dell'istituto, articoli di cronaca di giornali o quotidiani locali relativi ad eventi di cui la scuola è stata parte attiva.

Titolare e Responsabili del Trattamento:
Il titolare ed il Responsabile del trattamento sono puntualmente individuati nell'Informativa sulla Privacy, aggiornato ogni anno, e debitamente nominati.

Diritti dell'interessato:
In ogni momento potrà esercitare i Suoi diritti nei confronti del titolare del trattamento, ai sensi degli artt. da 15 a 22 e dell'art. 34 del GDPR.

Periodo di conservazione:
I dati raccolti verranno conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati ("principio di limitazione della conservazione", art.5, GDPR) e/o per il tempo necessario per obblighi di legge. La verifica sulla obsolescenza dei dati conservati in relazione alle finalità per cui sono stati raccolti viene effettuata periodicamente.

La presente liberatoria/autorizzazione è da ritenersi valida per tutto il periodo di permanenza del bambino/a presso l'Istituto e potrà essere revocata in ogni tempo con comunicazione scritta da inviare via posta comune o e-mail all' **Istituto Comprensivo Follonica 1**.

Data:_____ **Firma dell'interessato** (1) _____

Firma dell'interessato (2) _____

Nel caso di firma di un solo genitore

Il sottoscritto, consapevole delle conseguenze amministrative e penali per chi rilasci dichiarazioni non corrispondenti a verità ai sensi del DPR 245/2000, dichiara di aver effettuato la scelta/ richiesta in osservanza delle disposizioni sulla responsabilità genitoriale di cui agli art. 316, 338 ter e 337 quater del codice civile, che richiedono il consenso di entrambi i genitori.

Firma _____

Minori e foto su web

Il GDPR entrato in vigore il 25 maggio 2018 contiene anche linee guida su minori e foto su web.

Il garante conferma la necessità di un consenso da parte di entrambi i genitori, anche se separati o divorziati, al trattamento dei dati dei minori o alla loro divulgazione attraverso immagini o video.

In particolare, a pag.7 è scritto che *"I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore."*

COME DEVE COMPORTARSI LA SCUOLA
Premesso che è sempre un bene limitare le pubblicazioni online di minori, è indispensabile la firma di una liberatoria ben articolata (trasparenza, legittimità, proporzionalità) da parte di entrambi i genitori oltre alla fotocopia dei loro documenti.

È inoltre auspicabile:
evitare di riprendere singoli minori ma piuttosto utilizzare modalità gruppo dove quest'ultimo è ripreso almeno in secondo piano.

COME DEVONO COMPORTARSI I GENITORI
La pubblicazione di una fotografia online si inquadra nel trattamento di dati personali e sensibili, e costituisce interferenza nella vita privata del minore. In tal senso **occorre fare particolare attenzione nel pubblicare immagini di minori, anche se si tratta dei propri figli**. Nessuno vieta di pubblicare le foto dei propri figli sui social network (Facebook, Instagram, ecc.), tuttavia bisogna sapere che le immagini, soprattutto se accessibili a tutti possono essere utilizzate da chiunque e dovunque, senza possibilità di controllo.

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.

Gli studenti si impegnano a:

- utilizzare in modo consapevole e corretto la RETE e i dispositivi telematici, nel rispetto della privacy e della dignità propria e altrui;
- rispettare le consegne dei docenti;
- non scaricare materiali e software senza autorizzazione;
- non utilizzare unità removibili personali senza autorizzazione;
- 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;
- monitorare l'uso che gli studenti fanno delle tecnologie.

3.3 - Strumenti di comunicazione online

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

Relativamente agli ambienti di apprendimento il nostro istituto si avvale di:

n. 4 laboratori di informatica con circa 60 dispositivi digitali fissi e mobili;

n. LIM e digital board (Totale) 37.

Per la comunicazione interna vengono utilizzati i seguenti strumenti:

- registro elettronico che consente di gestire la comunicazione con le famiglie, che hanno la possibilità di essere costantemente informate interagendo direttamente con la scuola (andamento scolastico - assenze, argomenti lezioni e compiti, note disciplinari; risultati scolastici - voti, documenti di valutazione; prenotazione colloqui individuali; agenda eventi; comunicazioni varie);
- mail scolastica;
- piattaforma Google Meet e applicativi che ha favorito un lavoro collaborativo e condiviso rendendo possibile un più agevole passaggio alla didattica a distanza e le comunicazioni scuola-famiglia nel periodo di lockdown.

Riguardo alla comunicazione esterna il nostro Istituto utilizza il sito web costantemente aggiornato.

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.

Segue l'analisi delle indicazioni legislative sui dispositivi tecnologici nella loro evoluzione e le strategie che devono essere messe in atto a scuola con consapevolezza e responsabilità alla luce del quadro normativo e di indirizzo di riferimento.

La circolare n° 362 del 25 agosto 1998 "Uso del telefono cellulare nelle scuole" ha come oggetto particolare il divieto dell'uso del cellulare a scuola da parte dei docenti durante le ore di lezione; laddove si verifichi tale comportamento non può essere consentito, in quanto si traduce in una mancanza di rispetto nei confronti degli alunni e reca un obiettivo elemento di disturbo al corretto svolgimento delle ore di lezione che, per legge, "devono essere dedicate interamente all'attività di insegnamento e non possono essere utilizzate, sia pure parzialmente, per attività personali dei docenti".

La DM n. 30 del 15/03/2007 "Linee di indirizzo ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, doveri di vigilanza e di corresponsabilità dei genitori e dei docenti", invece, si concentra su più elementi che interessano, questa volta, anche gli studenti e le studentesse e ribadisce alcuni doveri contenuti nell'articolo 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", considerato che

il discente ha il dovere:

- di assolvere assiduamente agli impegni di studio anche durante gli orari di lezione (comma 1);
- di tenere comportamenti rispettosi nei confronti degli altri (comma 2), nonché corretti e coerenti con i principi di cui all'art. 1 (comma 3);
- di osservare le disposizioni organizzative dettate dai regolamenti di istituto (comma 4)".

Viene anche sottolineata l'importanza del Patto educativo di corresponsabilità condividendo diritti e doveri fra scuola e famiglia, la quale deve impegnarsi "a rispondere direttamente dell'operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone o alle strutture scolastiche o, più in generale, violino i doveri sanciti dal regolamento di istituto e subiscano, di conseguenza, l'applicazione di una sanzione anche di carattere pecuniario"; rimane invariata la responsabilità deontologica e professionale dei dirigenti, dei docenti e del personale ATA, che hanno il dovere di vigilare sui comportamenti degli studenti e delle studentesse il quale sussiste in tutti gli spazi scolastici e di segnalare eventuali infrazioni suscettibili di sanzioni disciplinari.

Nel D.P.R. del 21 Novembre 2007, n. 235 "Regolamento recante modifiche ed integrazioni al decreto del Presidente della Repubblica 24 giugno 1998, n. 249", concernente lo statuto delle studentesse e degli studenti della scuola secondaria, viene introdotto il Patto educativo di corresponsabilità (Art. 3) che definisce, attribuendole, le responsabilità fra istituzione scolastica e famiglia. Oggi, il Patto va letto anche in riferimento all'educazione dei ragazzi e delle ragazze all'uso dei nuovi dispositivi tecnologici, inclusi tablet e smartphone sia a scuola che a casa.

Con la DM n. 104 del 30/11/2007 "Linee di indirizzo e chiarimenti sulla normativa vigente sull'uso di telefoni cellulari e di altri dispositivi elettronici nelle comunità scolastiche" si chiarisce, anche in virtù della normativa allora vigente posta a tutela della privacy, il divieto di utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire e/o divulgare immagini, filmati o registrazioni vocali. In altre parole, è punibile sia a livello civile che penale (oltre che le sanzioni previste dagli artt. 3 e 4, D.P.R. 24 giugno 1998, n. 249 - "Regolamento recante lo statuto delle studentesse e degli studenti della scuola secondaria"), chi abusa dei dati personali altrui raccolti (immagini, filmati, registrazioni vocali…), violandone la privacy.

E proprio riguardo il Codice della Privacy, Digs. 196/2003, modificato e integrato dal D. Lgs. 101/2018 recependo il regolamento UE 2016/679 e art.10 del Codice Civile, è necessario considerare che "l'uso di cellulari e smartphone è in genere consentito per

fini strettamente personali, ad esempio per registrare le lezioni, e sempre nel rispetto delle persone. Spetta comunque agli istituti scolastici decidere nella loro autonomia come regolamentare o se vietare del tutto l'uso dei cellulari. Non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese. È bene ricordare che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere lo studente in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati. Stesse cautele vanno previste per l'uso dei tablet, se usati a fini di registrazione e non soltanto per fini didattici o per consultare in classe libri elettronici e testi on line".

La riproduzione dei dati deve, pertanto, rispondere alla sola esigenza di documentazione dell'attività didattica previa informativa e autorizzazione firmata o esplicito consenso (sono comprese le recite, i saggi scolastici e le gite raccolte dai genitori che non si configurano come violazione della privacy se raccolti per fini personali, familiari e non vengono pubblicate on line, in particolare sui social network).

A tal proposito, è bene ricordare la Legge n. 71 del 2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" che ancor di più cerca di contrastare manifestazioni comportamentali di soggetti minorenni a danno di altri minorenni che pongono "in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo" attraverso le tecnologie digitali. Dove anche gli adulti tutti, docenti e genitori, hanno responsabilità specifiche oltre che un ruolo di vigilanza e di educazione dei minori stessi.

La questione qui descritta è stata affrontata, per la prima volta in maniera integrata, nel Piano Nazionale Scuola Digitale emanato dal Miur con la Legge 107 del 2015: "al fine di sviluppare e di migliorare le competenze digitali degli studenti e di rendere la tecnologia digitale uno strumento didattico di costruzione delle competenze in generale, il Ministero dell'istruzione, dell'università e della ricerca adotta il Piano nazionale per la scuola digitale (...)".

L'attenzione verso le tecnologie digitali e il loro utilizzo in classe diventa così inclusivo e creativo, nel senso che 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.

In tal senso, gli smartphone, i tablet e i pc personali possono essere integrati nel lavoro nelle classi quando ben progettato e calibrato per discipline e obiettivi formativi e didattici.

A tale scopo, il MIUR, in collaborazione con AGID (l'Agenzia per il Digitale) e il Garante per la Privacy, ha elaborato apposite linee guida per promuovere il Bring your own device (BYOD), che apre alla didattica integrata tramite un uso dei propri dispositivi personali in classe e alla sicurezza delle interazioni e delle relazioni fra pari

tramite le tecnologie digitali. Come stabilito dall'autonomia scolastica, è nei singoli regolamenti d'Istituto che si inseriscono le sanzioni disciplinari in caso di uso scorretto dei cellulari da parte dei ragazzi e delle ragazze in classe.

Di seguito, i dieci i punti del Miur per l'uso dei dispositivi mobili a scuola, BYOD (Bring your own device):

1. Ogni novità comporta cambiamenti. Ogni cambiamento deve servire per migliorare l'apprendimento e il benessere delle studentesse e degli studenti e più in generale dell'intera comunità scolastica.

2. I cambiamenti non vanno rifiutati, ma compresi e utilizzati per il raggiungimento dei propri scopi. Bisogna insegnare a usare bene e integrare nella didattica quotidiana i dispositivi, anche attraverso una loro regolamentazione. Proibire l'uso dei dispositivi a scuola non è la soluzione. A questo proposito ogni scuola adotta una Politica di Uso Accettabile (PUA) delle tecnologie digitali.

3. La scuola promuove le condizioni strutturali per l'uso delle tecnologie digitali. Fornisce, per quanto possibile, i necessari servizi e l'indispensabile connettività, favorendo un uso responsabile dei dispositivi personali (BYOD). Le tecnologie digitali sono uno dei modi per sostenere il rinnovamento della scuola.

4. La scuola accoglie e promuove lo sviluppo del digitale nella didattica. La presenza delle tecnologie digitali costituisce una sfida e un'opportunità per la didattica e per la cultura scolastica. Dirigenti e insegnanti attivi in questi campi sono il motore dell'innovazione. Occorre coinvolgere l'intera comunità scolastica anche attraverso la formazione e lo sviluppo professionale.

5. I dispositivi devono essere un mezzo, non un fine. È la didattica che guida l'uso competente e responsabile dei dispositivi. Non basta sviluppare le abilità tecniche, ma occorre sostenere lo sviluppo di una capacità critica e creativa.

6. L'uso dei dispositivi promuove l'autonomia delle studentesse e degli studenti. È in atto una graduale transizione verso situazioni di apprendimento che valorizzano lo spirito d'iniziativa e la responsabilità di studentesse e gli studenti. Bisogna sostenere un approccio consapevole al digitale nonché la capacità d'uso critico delle fonti di informazione, anche in vista di un apprendimento lungo tutto l'arco della vita.

7. Il digitale nella didattica è una scelta: sta ai docenti introdurla e condurla in

classe. L'uso dei dispositivi in aula, siano essi analogici o digitali, è promosso dai docenti, nei modi e nei tempi che ritengono più opportuni.

8. Il digitale trasforma gli ambienti di apprendimento. Le possibilità di apprendere sono ampliate, sia per la frequentazione di ambienti digitali e condivisi, sia per l'accesso alle informazioni, e grazie alla connessione continua con la classe. Occorre regolamentare le modalità e i tempi dell'uso e del non uso, anche per imparare a riconoscere e a mantenere separate le dimensioni del privato e del pubblico.

9. Rafforzare la comunità scolastica e l'alleanza educativa con le famiglie. È necessario che l'alleanza educativa tra scuola e famiglia si estenda alle questioni relative all'uso dei dispositivi personali. Le tecnologie digitali devono essere funzionali a questa collaborazione. Lo scopo condiviso è promuovere la crescita di cittadini autonomi e responsabili.

10. Educare alla cittadinanza digitale è un dovere per la scuola. Formare i futuri cittadini della società della conoscenza significa educare alla partecipazione responsabile, all'uso critico delle tecnologie, alla consapevolezza e alla costruzione delle proprie competenze in un mondo sempre più connesso.

In tale ottica, occorre integrare i Regolamenti già esistenti per disciplinare l'utilizzo delle TIC all'interno della scuola (es. la dotazione di filtri), prevedere misure per prevenire diverse tipologie di rischio (non solo quelle più frequenti come il cyberbullismo) e stabilire procedure specifiche per rilevare e gestire le diverse problematiche.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023).

- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity).

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

- 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.*

Come sappiamo, le dimensioni che il fenomeno può determinare sono molteplici e riconducono alla capacità di gestione di dinamiche complesse, mediante confronto/relazione con il Sé e l'altro, dimensioni dell'affettività e, ancora, mediante il riconoscimento di un limite tra dimensione di legalità ed utilizzo sicuro delle tecnologie digitali.

Per questo motivo la scuola intende perseguire azioni per rispondere ai bisogni dell'utenza, attraverso una risposta integrata con la rete dei servizi territoriali locali (tra cui ASL, Polizia postale, etc.).

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

Quando si parla di rischio in questo caso si fa riferimento alla 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.

La necessità di sensibilizzare ad un uso positivo e consapevole delle TIC gli studenti e le studentesse, sia in un'ottica di tutela dai rischi potenziali che di valorizzazione delle opportunità esistenti, pone la scuola ed i genitori di fronte alla sfida di riconsiderare la propria identità, il proprio ruolo educativo e le proprie risorse, oltre allo stato dei rapporti reciproci per un patto educativo da rinnovare costantemente.

La prima responsabilità degli insegnanti consiste, dunque, nell'imparare a riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente.

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.

Due sono i principali strumenti in questo caso da mettere in campo e si sintetizzano in interventi di Sensibilizzazione e Prevenzione.

Parlando di prevenzione in ambito digitale si potrebbe tradurre quanto appena detto con 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.

1.

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, legato 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 con la rete dei servizi locali (in primis le ASL e la Polizia Postale).

Inoltre, la responsabilità dell'azione preventiva ed educativa chiama in campo diverse agenzie educative oltre alla scuola, come la famiglia, ma non solo (istituzioni, associazioni, società civile, etc.), ciascuna con un proprio compito nei confronti di bambini e bambine e di adolescenti. Tali agenzie sono chiamate a collaborare ad un progetto comune, nell'ambito di funzioni educative condivise.

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).

Le caratteristiche del cyberbullismo

I tratti specifici del bullismo online sono correlati all'impatto che le tecnologie digitali hanno nella vita dei ragazzi e alle caratteristiche stesse della Rete e sono i seguenti (Willard, N., Educator's guide to cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress, Research Press, Illinois, 2005):

- l'impatto: la diffusione di materiale tramite Internet è incontrollabile e non è possibile prevederne i limiti (anche se la situazione migliora, video e immagini potrebbero restare online e continuare a diffondersi). Un contenuto offensivo e denigratorio online può, quindi, diventare virale e distruggere in alcuni casi la reputazione della vittima;

- la convinzione dell'anonimato: chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile. Sentendosi protetti dall'anonimato ci si sente liberi e più forti nel compiere atti denigratori, senza il timore di essere scoperti. È importante tenere bene a mente, però, che quello dell'anonimato è un "falso mito della Rete". Ogni nostra azione online è, infatti, rintracciabile e riconducibile a noi con gli strumenti opportuni o con l'intervento della Polizia Postale;

- l'assenza di confini spaziali: il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo dei suoi spazi-rifugio. La vittima può essere raggiungibile anche a casa e vive nella costante percezione di non avere vie di fuga. Spegnere il cellulare o il computer non basta, così come cancellare tutti i propri profili social. Il solo pensiero che eventuali contenuti denigratori continuino a diffondersi online è doloroso e si accompagna ad un senso costante di rabbia e impotenza;

- l'assenza di limiti temporali: può avvenire a ogni ora del giorno e della notte;

- l'indebolimento dell'empatia: esistono cellule chiamate neuroni specchio che ci permettono di "leggere" gli altri quando li abbiamo di fronte, capirli e di provare emozioni simile a quelle che loro provano, proprio come se fossimo di fronte ad uno specchio. Tale sensazione è data dall'attivazione di una particolare area del cervello. Quando le interazioni avvengono prevalentemente online la funzione speciale di questi neuroni viene meno (mancando la presenza fondamentale dell'altro che è sostituito dal dispositivo). La riduzione di empatia che ne consegue può degenerare nei comportamenti noti messi in atto dai cyberbulli;

- il feedback non tangibile: il cyberbullo non vede in modo diretto le reazioni della vittima e, ancora una volta, ciò riduce fortemente l'empatia e il riconoscimento del danno provocato.

Occorre tenere presente che il cyberbullo non è mai del tutto consapevole della gravità dei suoi comportamenti se non viene aiutato ad esserne consapevole. Inoltre, il cyberbullismo non lascia segni fisici evidenti sulla vittima e si consuma in un contesto virtuale che spesso viene percepito dai ragazzi come non "reale", come un mondo ludico a sé stante.

La mediazione tecnologica, infatti, porta ad un certo distanziamento fra aggressore e vittima, causando quello che Bandura ha definito come "disimpegno morale". Si tratta di un indebolimento del controllo morale interno dell'individuo, con la conseguente minimizzazione delle responsabilità individuali. Tale fenomeno vale non solo per il cyberbullo, ma anche per i cosiddetti bystander, ossia coloro che sono spettatori dei fatti.

A ciò si aggiungono altre convinzioni o tendenze frequenti nell'uso della Rete:

- percezione che online non ci siano norme sociali da rispettare: fra i giovani spesso vige la falsa convinzione secondo cui la Rete sia uno spazio virtuale lontano dalla realtà, in cui vige libertà assoluta e in cui regole e norme sociali della vita quotidiana non valgono;

- la sperimentazione online di identità e personalità multiple: la Rete è per i minori il luogo virtuale per eccellenza in cui mettersi in gioco “fingendo di essere ciò che non si è” per il semplice gusto di sperimentare nuove forme di identità e comportamento;

- il contesto virtuale come un luogo di simulazione e giochi di ruolo: “la vita sullo schermo” e tutti i comportamenti messi in atto online vengono percepiti solo come un gioco;

- diffusione di responsabilità: tutti quelli che partecipano anche solo con un like o un commento diventano, di fatto, corresponsabili delle azioni del cyberbullo facendo accrescere la portata dell’azione.

Gli atti di cyberbullismo possono essere suddivisi in due gruppi:

cyberbullismo diretto: il bullo utilizza strumenti di messaggistica istantanea (es. sms, mms) che hanno un effetto immediato sulla vittima, poiché diretti esclusivamente alla persona;

cyberbullismo indiretto: il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima anche da un punto di vista psicologico.

Indicatori di segnali che può manifestare una potenziale vittima di cyberbullismo sono:

- appare nervosa quando riceve un messaggio o una notifica;

- sembra a disagio nell’andare a scuola o finge di essere malata (ha spesso mal di stomaco o mal di testa);

- cambia comportamento ed atteggiamento in modo repentino;

- mostra ritrosia nel dare informazioni su ciò che fa online;

- soprattutto dopo essere stata online, mostra rabbia o si sente depressa;

- inizia ad utilizzare sempre meno Pc e telefono (arrivando ad evitarli);

- perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;

- il suo rendimento scolastico peggiora.

La normativa in materia

Il Parlamento italiano ha approvato il 18 maggio 2017 la Legge 71/2017, "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", una legge a tutela dei minori per la prevenzione e il contrasto al cyberbullismo, che prevede misure prevalentemente a carattere educativo/rieducativo. La legge pone al centro il ruolo dell'istituzione scolastica nella prevenzione e nella gestione del fenomeno e ogni Istituto scolastico dovrà provvedere ad individuare fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo. Questi aspetti vengono chiariti nel dettaglio dalle Linee di orientamento per la prevenzione e il contrasto del cyberbullismo.

La L.71/17 introduce per la prima volta nell'ordinamento giuridico anche una definizione di cyberbullismo (come già riportato sopra).

Nella consapevolezza che le azioni efficaci siano quelle che ricorrono agli strumenti educativi, rieducativi e di mediazione del conflitto, esistono tuttavia responsabilità da conoscere, la possibilità di commettere reati o danni civili e specifici dispositivi giuridici.

Sempre la Legge 71/2017 introduce un provvedimento di carattere amministrativo per gli autori di atti di cyberbullismo, la procedura di ammonimento da parte del Questore: il minore autore può essere convocato dal Questore e ammonito se ritenuto responsabile delle azioni telematiche.

Più precisamente, la procedura di ammonimento prevista in materia di stalking (art. 612-bis c.p.), in caso di condotte di ingiuria (art. 594 c.p.), diffamazione (art. 595 c.p.), minaccia (art. 612 c.p.) e trattamento illecito di dati personali (art. 167 del codice della privacy) commessi mediante internet da minori ultraquattordicenni (nel nostro ordinamento l'imputabilità penale, ossia la responsabilità personale per i reati commessi, scatta al quattordicesimo anno, in relazione al raggiungimento della cosiddetta "capacità d'intendere e volere") nei confronti di altro minorenne, se non c'è stata querela o non è stata presentata denuncia, è stata estesa al cyberbullismo e può essere impartita da parte del questore (il questore convoca il minore, insieme ad almeno un genitore o a chi esercita la responsabilità genitoriale). Gli effetti dell'ammonimento cessano al compimento della maggiore età.

Chi compie atti di bullismo e cyberbullismo può anche essere responsabile di reati penali e danni civili.

Secondo il codice penale italiano i comportamenti penalmente rilevanti in questi casi sono:

- percosse (art. 581);

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

Nei casi più gravi, basta la denuncia ad un organo di polizia o all'autorità giudiziaria per attivare un procedimento penale (per es. lesioni gravi, minaccia grave, molestie); negli altri casi, la denuncia deve contenere la richiesta che si proceda penalmente contro l'autore di reato (querela).

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

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

- I genitori, perché devono educare adeguatamente e vigilare, in maniera adeguata all'età del figlio, cercando di correggerne comportamenti devianti. Questa responsabilità generale persiste anche per gli atti compiuti nei tempi di affidamento alla scuola (culpa in educando), così come previsto dal Codice civile. Se i genitori riescono a fornire la prova di aver fatto di tutto per impedire il fatto e considerata l'imprevedibilità e repentinità, in concreto dell'azione dannosa, possono essere esonerati dall'obbligo di risarcire il danno causato dal figlio. Non c'è responsabilità penale dei genitori, perché la responsabilità penale è personale.

- Gli insegnanti e la scuola: perché nei periodi in cui il minore viene affidato all'Istituzione scolastica il docente è responsabile della vigilanza sulle sue azioni (ore di attività didattiche, ricreazione, pausa pranzo, palestra, uscite didattiche e viaggi d'istruzione) e ha il dovere di impedire comportamenti dannosi verso gli altri/e ragazzi/e, insegnanti e personale scolastico o verso le strutture della scuola stessa (culpa in vigilando art. 2048 del Codice Civile, responsabilità dei precettori). La responsabilità dei docenti si estende anche a viaggi, gite scolastiche, manifestazioni sportive organizzate dalla scuola.

Di questa colpa/responsabilità i docenti possono essere liberati dimostrando di non aver potuto impedire il fatto. Si tiene conto in questi casi dell'età e del grado di maturità dei ragazzi, della concreta situazione ambientale, etc.

Inoltre, l'insegnante deve dimostrare di aver adottato in via preventiva le misure idonee ad evitare la situazione di pericolo.

A pagare in primis sarà la scuola, che di surroga al suo personale nelle responsabilità

civili derivanti da azioni giudiziarie promosse da terzi, fermo restando che poi potrà rivalersi sul singolo insegnante per dolo o colpa grave (art. 61 della L. n. 312/1980, responsabilità patrimoniale del personale direttivo, docente educativo e non docente).

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

Iniziative di intervento

La Legge 71/2017 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).

Qualora ci si trovi di fronte ad un caso di cyberbullismo si dovrà:

- informare i genitori degli alunni coinvolti;

- coinvolgere il referente di istituto dell'e-safety e gli operatori scolastici su quanto sta accadendo;
- coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online;
- tenere traccia di quanto successo e delle azioni intraprese, compilando un "diario di bordo" per consentire ulteriori indagini se necessarie.
- mettere in atto azioni condivise tra scuola e famiglia al fine di intervenire preventivamente ed efficacemente, per evitare, arginale ed eliminare possibili manifestazioni di comportamenti antisociali.

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.

Lo scorso A.S. il nostro Istituto ha sottoscritto accordo di rete con validità triennale fra Istituti Comprensivi e Istituti Superiori della Provincia di Grosseto, in costante e continua collaborazione con l'Ufficio Scolastico Territoriale, con ruolo di scuola-capofila svolto dall'Istituto Polo Bianciardi (Gr). La rete ricerca le seguenti finalità condivise:

- accrescere competenze e conoscenze dei docenti, dei Referenti d'istituto e dei Referenti territoriali sulle tematiche oggetto della rete: bullismo e cyberbullismo;
- promuovere campagne informative sul territorio, raccogliere e documentare buone pratiche;
- realizzare Linee guida d'azione e d'intervento per affrontare i casi che si verificano all'interno delle scuole;
- promuovere forme permanenti di collaborazione sul territorio della provincia di Grosseto con il coinvolgimento e la partecipazione di più soggetti interessati, attraverso lo strumento del "Protocollo d'Intesa";

- creare una Piattaforma operativa, con individuazione fi un gruppo di gestione e di lavoro, nella quale inserire documenti e materiali. Tale piattaforma potrà essere suddivisa in Aree Tematiche quali, a titolo di esempio: normativa, definizione dei termini, casistica, statistiche. Inoltre potrà contenere progetti ed iniziative proposti da enti esterni, progetti ed iniziative attuate dalle scuole della provincia di Grosseto, attività di formazione rivolta a docenti, studenti e genitori, raccolta di risorse multimediali;

- creare uno spazio aperto nelle modalità di pagina social o blog, nel quale poter interagire con la cittadinanza per ascoltare dubbi e chiarimenti, fornire aiuto e supporto. L'organizzazione delle risorse umane, in tal caso, dovrebbe comprendere una varietà di profili professionali che possano dare un contributo secondo le proprie competenze e conoscenze.

A seguito di tale accordo di rete verrà realizzato nell'A.S. 2022/23 un progetto per la prevenzione, la sensibilizzazione e il contrasto al cyberbullismo dal titolo "La tua vita non è un hastag: utilizziamo la rete in modo consapevole". Il progetto (Ufficio Scolastico Regionale per la Toscana - Avviso pubblico per l'assegnazione di fondi da destinare alle istituzioni scolastiche o reti finanziarie scuole per progetti dedicati al contrasto al cyberbullismo ai sensi della L. 234/2021, commi 671 e 672) strutturato in modo verticale con il coinvolgimento di più ordini di scuole, mette gli alunni al centro dell'apprendimento e mira al coinvolgimento in modo ampio e articolato tutti i membri della comunità scolastica.

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.

Data l'importanza di questa tematica l'Istituto promuoverà interventi di formazione degli studenti e delle studentesse tenuti dai docenti e da esperti esterni (forze dell'ordine, psicologi, personale sanitario...).

Occorre valorizzare la dimensione relazionale dei più giovani, sensibilizzandoli verso capacità di analisi e discernimento, per fornire strumenti idonei, tanto comunicativi quanto educativi sotto l'aspetto civico e morale.

La corresponsabilità con la famiglia è un precursore fondamentale nell'azione didattico-educativa della scuola, anche per attivare progettazioni complementari con finalità socio-educative.

Le caratteristiche dell'hate speech (fonte documento No hate Ita):

1. Il discorso d'odio procura sofferenza. La parola ferisce, e a maggior ragione l'odio! Il discorso può violare i diritti umani. Il discorso d'odio online non è meno grave della sua espressione offline, ma è più difficile da individuare e da combattere.

2. Gli atteggiamenti alimentano gli atti. Il discorso dell'odio è pericoloso anche perché può condurre a più gravi violazioni dei diritti umani, e perfino alla violenza fisica. Può contribuire a inasprire le tensioni razziali e altre forme di discriminazione e di violenza.

3. L'odio online non è solo espresso a parole. Internet ci permette di comunicare rapidamente e in modi svariati, ad esempio, mediante i social media e i giochi online, molto spesso, d'altronde, in maniera anonima. L'odio online può esprimersi sotto forma di video e foto, come pure, più solitamente, di contenuto testuale. Le forme visive o multimediali hanno sovente un impatto più forte sugli atteggiamenti (consci e inconsci).

4. L'odio prende di mira sia gli individui che i gruppi. L'odio online può prendere di mira dei gruppi che spesso sono già vulnerabili sotto altri aspetti, come i richiedenti asilo, le minoranze religiose o le persone con disabilità. Tuttavia, anche i singoli individui sono sempre maggiormente oggetto di attacchi. Le

conseguenze sono talvolta fatali, come dimostrato da numerosi fatti di cronaca riferiti dai media, riguardanti giovani vittime di cyberbullismo che sono state spinte al suicidio.

5. Internet è difficilmente controllabile. La diffusione di messaggi di incitamento all'odio è maggiormente tollerata su Internet rispetto al mondo offline ed è sottoposta a minori controlli. È ugualmente più facile (e comporta meno rischi) insultare o molestare online, perché le persone spesso si esprimono sotto la copertura dell'anonimato.

6. Ha radici profonde. Gli atteggiamenti e le tensioni sociali che suscitano sentimenti di odio online affondano le loro radici nella società, e non sono diversi, in genere, da quelli che alimentano il discorso dell'odio offline.

7. Impunità e anonimato. Sono le due presunte caratteristiche delle interazioni sociali in rete: l'impunità e l'anonimato. Queste abbassano le remore etiche. In realtà, però, qualsiasi azione compiuta sul web consente di rintracciare il suo autore.

Sotto il profilo educativo si potrebbe pensare ad attività di analisi e produzione mediale, finalizzate soprattutto a:

- 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.

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

Dominanza. L'attività domina i pensieri ed il comportamento del soggetto, assumendo un valore primario tra tutti gli interessi.

Alterazioni del tono dell'umore: l'inizio dell'attività provoca cambiamenti nel tono dell'umore. Il soggetto prova un aumento d'eccitazione o maggiore rilassatezza come diretta conseguenza dell'incontro con l'oggetto della dipendenza.

Conflitto: conflitti inter-personali tra il soggetto e coloro che gli sono vicini, conflitti intra-personali interni a se stesso, a causa del comportamento dipendente.

Ricaduta: tendenza a ricominciare l'attività dopo averla interrotta.

I segnali patologici di questo che viene descritto come "un vero e proprio abuso della tecnologia", anche denominato "Internet Addiction Disorder" (I.A.D. coniato dallo psichiatra Ivan Goldberg 1996), sono specifici così come accade per le altre dipendenze più "tradizionali". In particolare, si hanno: la tolleranza ossia quando vi è un crescente bisogno di aumentare il tempo su internet e l'astinenza quando, cioè, vi è l'interruzione o la riduzione dell'uso della Rete che comporta ansia, agitazione psicomotoria, fantasie, pensieri ossessivi (malessere psichico e/o fisico che si manifesta quando s'interrompe o si riduce il comportamento). Tutto questo ha ripercussioni sulla sfera delle relazioni interpersonali che diventano via via più povere e alle quali si preferisce il mondo virtuale, con alterazioni dell'umore e della percezione del tempo.

Da sottolineare, la nomofobia (nomo deriva da "no-mobile") termine usato per categorizzare quei soggetti che sperimentano emozioni negative, quali ansia, tristezza e rabbia quando non sono connessi con il proprio smartphone.

Di seguito i sintomi che devono essere presenti :

1. il giocatore è assorbito totalmente dal gioco;
2. il giocatore è preoccupato e ossessionato dal gioco;
3. il gioco consente alla persona di sfuggire alla realtà con la sperimentazione di emozioni più piacevoli;
4. il giocatore manifesta sempre di più l'impulso di giocare e di sperimentare emozioni positive;

5. il giocatore sente di dover dedicare più tempo ai giochi;
6. il giocatore se non può giocare manifesta ansia, depressione e irritabilità;
7. può emergere un ritiro sociale (si veda il punto 3);
8. il giocatore, anche se comprende la gravità della situazione e sospende di giocare comunque non riesce a interrompere del tutto;
9. il giocatore mente agli altri sull'utilizzo che fa dei giochi on line;
10. il giocatore ha perso o mette a rischio relazioni o opportunità a causa dei giochi su Internet o ha perso interesse verso attività nella vita reale.

La scuola intende favorire il benessere digitale ed in particolare:

- 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).

4.5 - Sexting

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

La Legge 19 luglio 2019 n. 69, all'articolo 10, ha introdotto in Italia il reato di "revenge porn" (letteralmente significa "vendetta del porno"), ossia la diffusione illecita di immagini o di video sessualmente espliciti.

Tra le caratteristiche del fenomeno vi sono principalmente:

la fiducia tradita: chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo, inoltre, alla motivazione della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale);

la pervasività con cui si diffondono i contenuti: in pochi istanti e attraverso una condivisione che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso a un numero esponenziale e infinito di persone e ad altrettante piattaforme differenti. Il contenuto, così, diventa facilmente modificabile, scaricabile e condivisibile e la sua trasmissione è incontrollabile;

la persistenza del fenomeno: il materiale pubblicato online può permanervi per un tempo illimitato e potrebbe non essere mai definitivamente rimosso. Un contenuto ricevuto, infatti, può essere salvato, a sua volta re-inoltrato oppure condiviso su piattaforme diverse da quelle originarie e/o in epoche successive.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psico-sessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'Altro e depressione.

Questi comportamenti hanno ripercussioni negative sulla vittima in termini di autostima, di credibilità, di reputazione sociale off e on line.Qualora ci si trovi di fronte a un caso di sexting (con cui si intende l'invio e/o la ricezione e/o la condivisione di testi, video o immagini sessualmente esplicite via cellulare o tramite internet) si dovrà:

- coinvolgere la classe e confrontarsi con esperti, facendo appello, per esempio, ad eventuali sportelli d'ascolto per capire come approfondire e affrontare il fenomeno;
- coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti riconducibili al sexting;
- intraprendere con la classe attività mirate a riflettere sulla fiducia che ciascuno ripone negli altri e sul fenomeno del sexting.

4.6 - Adescamento online

Il ***grooming*** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione

intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

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

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

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

Per riconoscere un eventuale caso di adescamento online è importante prestare attenzione a piccoli segnali che possono essere indicatori importanti, per valutare un cambiamento improvviso nel comportamento di un minore. A seguire alcuni segnali e domande che potrebbero essere di aiuto:

- il minore ha conoscenze sessuali non adeguate alla sua età?
- viene a conoscenza di un certo video o di una foto che circola online o il minore ha ricevuto un contenuto (o filmato), ma c'è imbarazzo e preoccupazione nel raccontarvi di più…
- il minore si isola totalmente e sembra preso solo da una relazione online?
- ci sono prese in giro e allusioni sessuali verso un bambino/ragazzo in particolare?

L'adescamento non avviene apparentemente con una dinamica violenta, ma il "prendersi cura" del minore rappresenta la conditio per carpirne la fiducia ed instaurare una relazione a sfondo erotico. Può capitare che l'adescatore si presenti al minore sotto falsa identità, fingendo quindi di essere un'altra persona così da attirare maggiormente l'attenzione del minore (ad esempio, potrebbe fingersi un talent scout del mondo dello spettacolo alla ricerca di volti nuovi).

Potenziali vittime dell'adescamento online possono essere sia bambini che bambine,

sia ragazzi che ragazze. Il fenomeno, infatti, non conosce distinzione di genere. Gli adolescenti sono particolarmente vulnerabili, poiché si trovano in una fase della loro vita in cui è molto importante il processo di costruzione dell'identità sessuale. Anche per questo potrebbero essere aperti e curiosi verso nuove esperienze e, talvolta, attratti da relazioni intime e apparentemente rassicuranti.

Le tecnologie digitali consentono ai giovani di ampliare la propria rete di amicizie in modo quasi smisurato; questo li espone a rischi notevoli, come quello di dare accesso a sconosciuti al loro mondo online e quindi a informazioni personali.

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.

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 (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è).

È bene che anche gli insegnanti aiutino i propri alunni a tutelarsi, scegliendo con cura chi frequentare online, per evitare che una condotta imprudente possa comportare ripercussioni non banali nella loro vita reale. Una volta riconosciuti alcuni segni che possono rinviare a una situazione di adescamento online, quali un improvviso calo nel rendimento scolastico; un aumento del tempo trascorso dall'alunno online congiunto ad una particolare riservatezza al riguardo; allusioni da parte dell'alunno alla frequentazione di una persona più grande, o a regali ricevuti, ecc., è bene:

- approfondire la situazione coinvolgendo la classe e l'intera comunità scolastica;
- avviare dei percorsi di riflessione in classe sul concetto di fiducia;
- farsi affiancare da esperti (Forze dell'ordine, personale sanitario, psicologo) ricorrendo anche allo sportello d'ascolto per offrire ai minori, qualora lo desiderino, il supporto necessario.

4.7 - Pedopornografia

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

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

bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

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

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

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

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

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

L'Istituto realizzerà un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico, promuovendo il Vademecum di Generazioni Connesse, una guida operativa, che ha l'obiettivo di diffondere, soprattutto a livello territoriale, strumenti conoscitivi ed operativi utili per orientarsi nelle gestione di alcune problematiche inerenti l'uso delle TIC.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023).

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

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

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

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

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

☐ 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.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i 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 il contenuto entro 48 ore.

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.

In relazione al CASO A, è opportuno il coinvolgimento del Referente d'Istituto per il contrasto del bullismo e del cyberbullismo, al fine di valutare le possibili strategie d'intervento. Se si ravvisano gli estremi, viene informato il Dirigente scolastico unitamente al Consiglio di classe.

Uno strumento utile per raccogliere informazioni può essere il diario di bordo (allegato alla presente e-Policy): il docente deve cercare di capire se gli episodi sono circoscritti al gruppo o se interessano l'intero Istituto. Operativamente è fondamentale coinvolgere tutti gli studenti e le studentesse, informandoli sui fenomeni e sulle caratteristiche degli stessi, suggerendo di chiedere aiuto se pensano di vivere situazioni, di subire atti identificabili come bullismo o cyberbullismo.

In relazione al CASO B, il docente deve condividere immediatamente quanto osservato con il Referente per il bullismo e il cyberbullismo, al fine di valutare insieme le possibili strategie di intervento. Si avvisa anche il Dirigente Scolastico che eventualmente convoca il Consiglio di classe. Se non si ravvisano fattispecie di reato, è opportuno:

- informare i genitori (o chi esercita la responsabilità genitoriale) degli/delle studenti/studentesse direttamente coinvolti/e (qualsiasi ruolo abbiano avuto), se possibile con la presenza di professionisti dell'aiuto, per strategie condivise e modalità di supporto;
- creare momenti di confronto costruttivo in classe, con la presenza di figure specialistiche territoriali;
- informare i genitori degli/delle studenti/studentesse infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy);
- informare gli/le studenti/studentesse ultra quattordicenni della possibilità di

richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o Social (o successivamente, in caso di non risposta, al garante della Privacy);

- convocare il consiglio di classe;
- valutare come coinvolgere gli operatori scolastici su quello che sta accadendo.

A seconda della situazione e delle valutazioni effettuate con Referente, Dirigente e genitori, si potrebbe poi segnalare alla Polizia Postale, ove necessario ai sensi di legge:

- contenuto del materiale online offensivo;
- modalità di diffusione;
- fattispecie di reato eventuale.

Se è opportuno, richiedere un sostegno ai servizi e alle associazioni territoriali o ad altre autorità competenti (pensiamo al cyberbullismo, con il suo impatto sulla vita quotidiana della vittima, la quale sa che i contenuti lesivi sono online, diffusi fra molte persone conosciute e non, in un circuito temporale senza fine e senza barriere spaziali).

E' bene sempre dialogare con la classe, attraverso interventi educativi specifici, cercando di sensibilizzare studenti e studentesse sulla necessità di non diffondere ulteriormente online i materiali dannosi, ma anzi di segnalarli e bloccarli. Ciò è utile anche per capire il livello di diffusione dell'episodio all'interno dell'Istituto.

Strumenti a disposizione di studenti/esse per le segnalazioni a scuola

Per aiutare gli/le studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni si potrebbero prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo 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.

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.

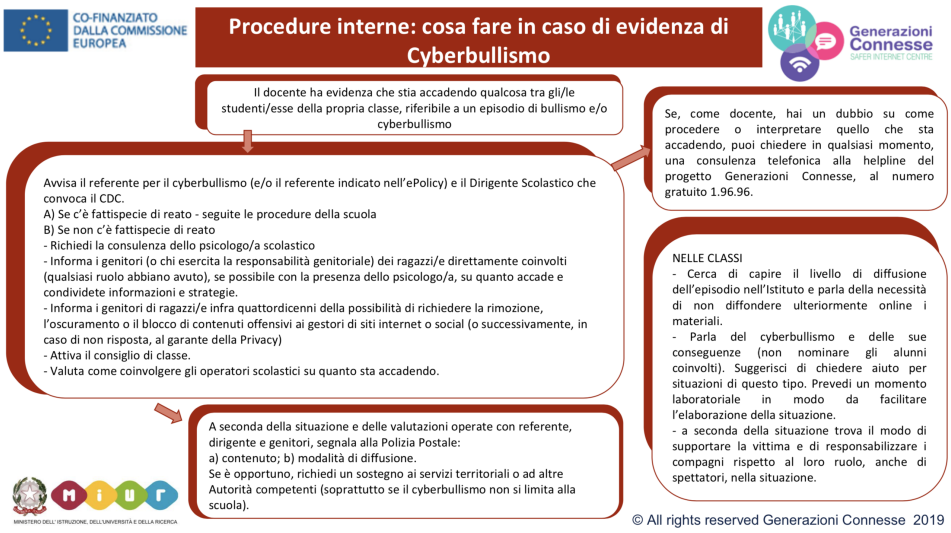
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

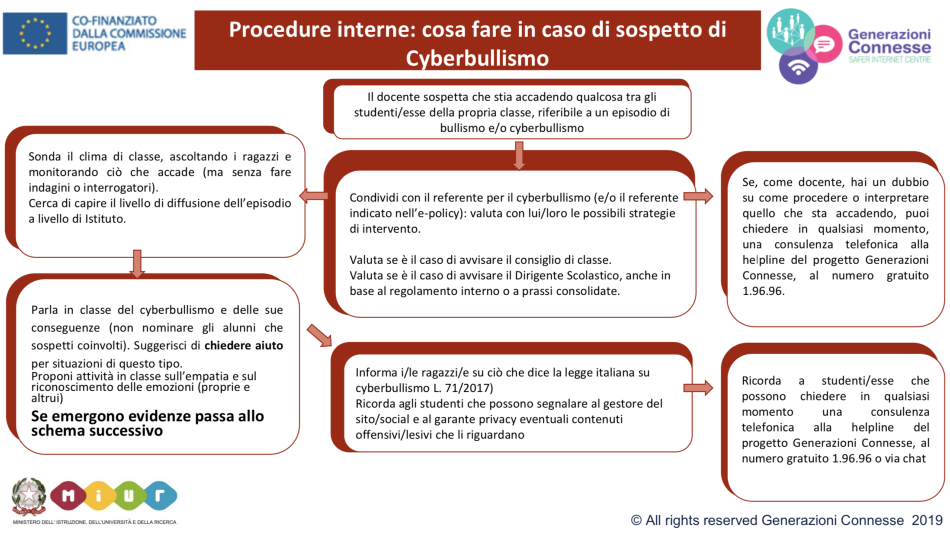
Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;

Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

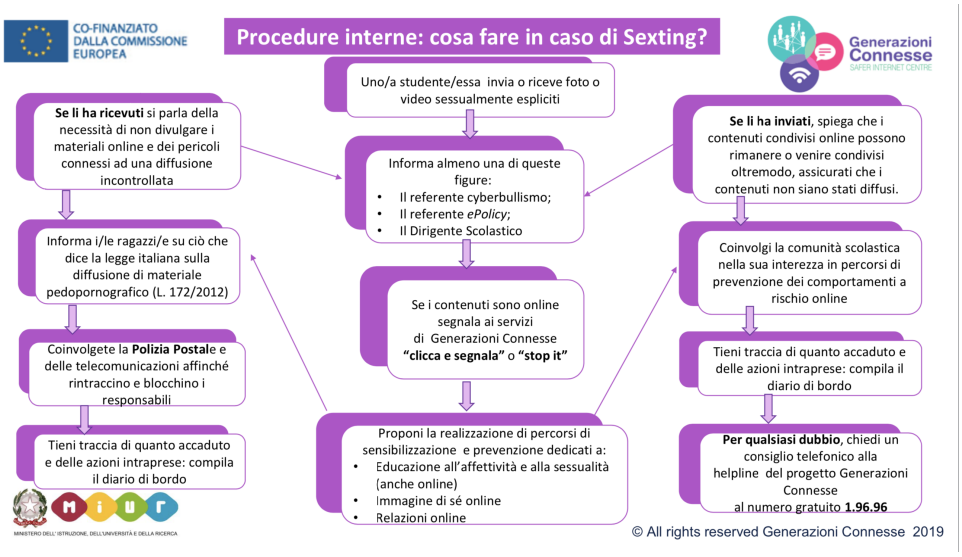
5.4. - Allegati con le procedure

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

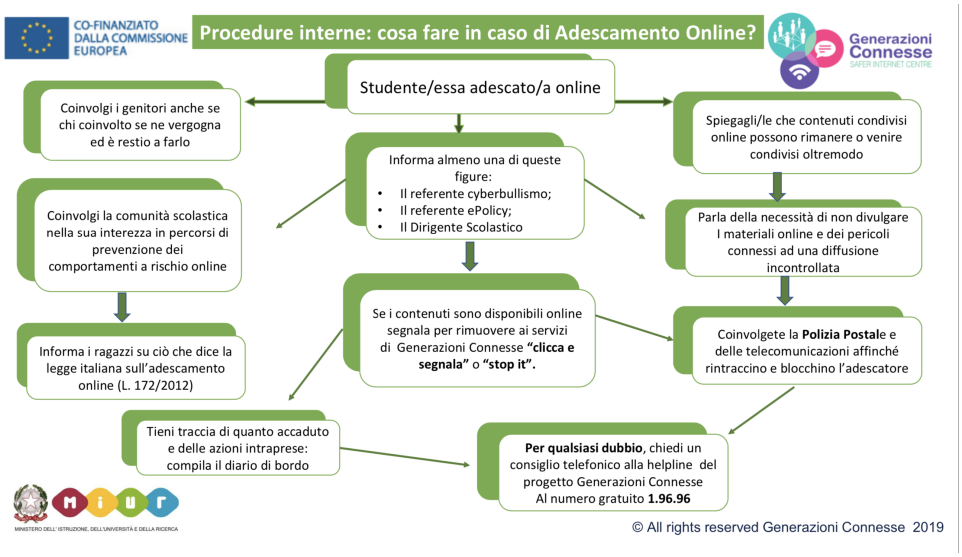




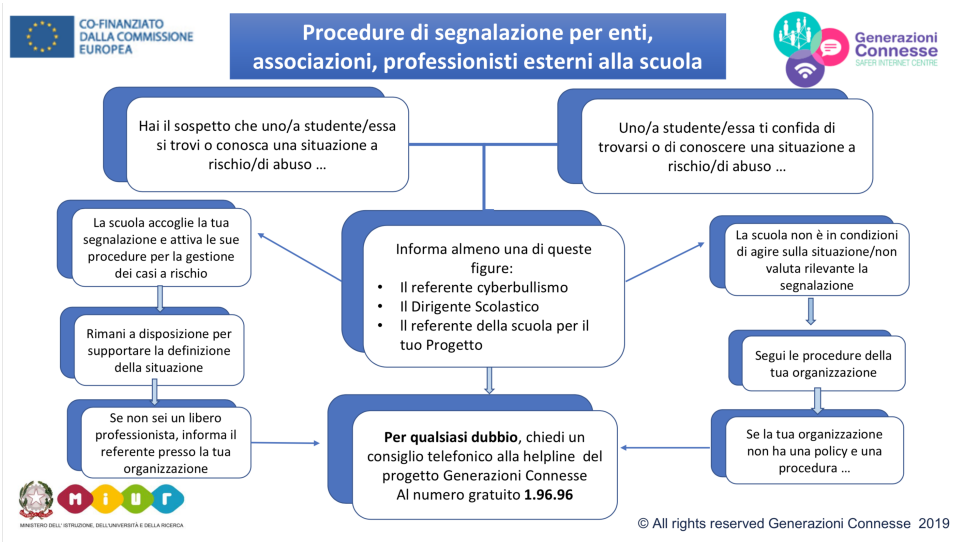
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



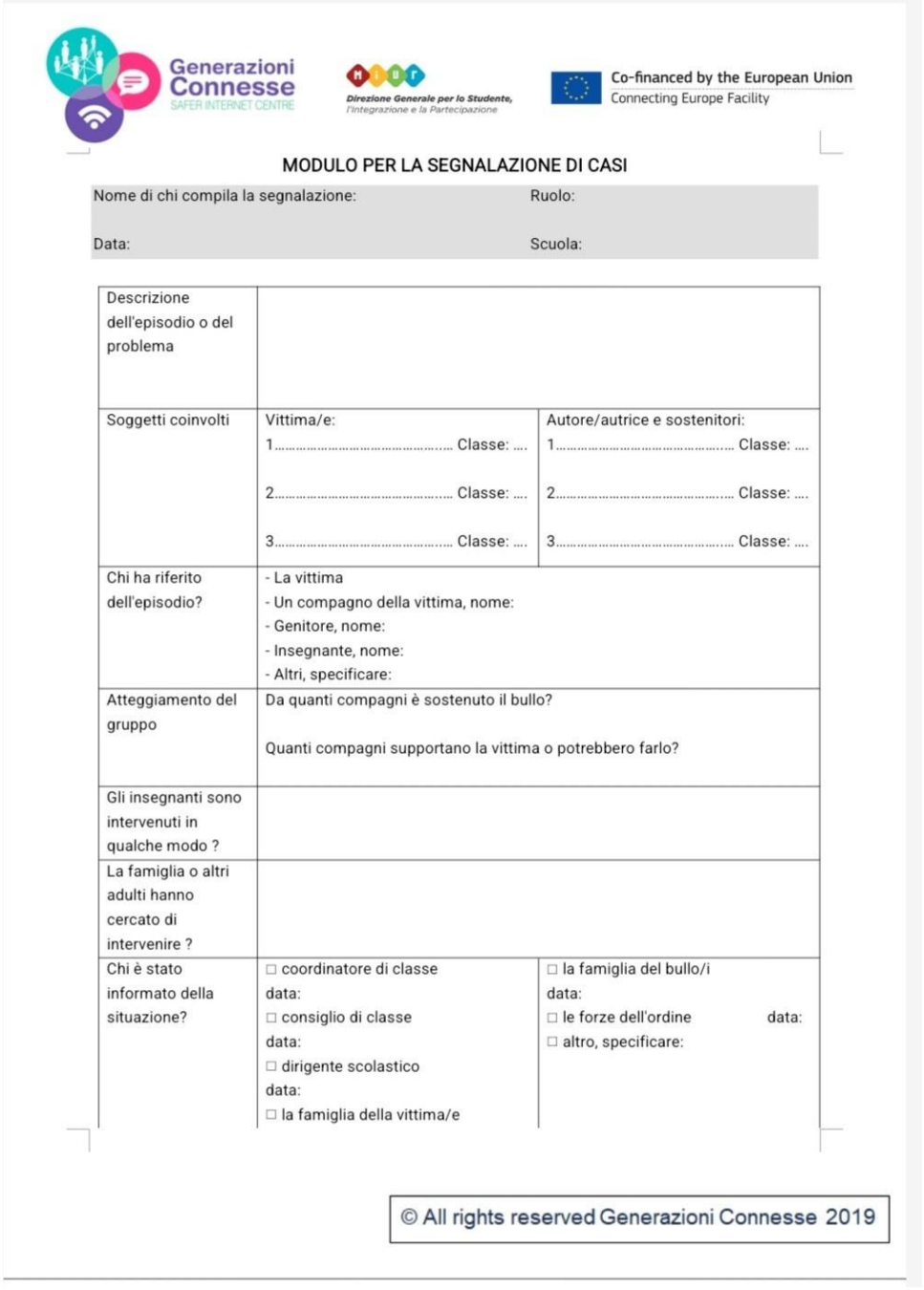
Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola



Altri allegati

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

Si aggiungono, di seguito, modulistica utile per la segnalazione/gestione di casi, glossario e scheda di approfondimento.



Generazioni Connesse
SAFER INTERNET CENTRE

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

Co-financed by the European Union
Connecting Europe Facility

MODULO PER LA SEGNALAZIONE DI CASI

Nome di chi compila la segnalazione:	Ruolo:
Data:	Scuola:

Descrizione dell'episodio o del problema		
Soggetti coinvolti	Vittima/e: 1..... Classe: .... 2..... Classe: .... 3..... Classe:	Autore/autrice e sostenitori: 1..... Classe: .... 2..... Classe: .... 3..... Classe: ....
Chi ha riferito dell'episodio?	- La vittima - Un compagno della vittima, nome: - Genitore, nome: - Insegnante, nome: - Altri, specificare:	
Atteggiamento del gruppo	Da quanti compagni è sostenuto il bullo? Quanti compagni supportano la vittima o potrebbero farlo?	
Gli insegnanti sono intervenuti in qualche modo ?		
La famiglia o altri adulti hanno cercato di intervenire ?		
Chi è stato informato della situazione?	☐ coordinatore di classe data: ☐ consiglio di classe data: ☐ dirigente scolastico data: ☐ la famiglia della vittima/e	☐ la famiglia del bullo/i data: ☐ le forze dell'ordine data: ☐ altro, specificare:

	data:	

MODULO PER IL FOLLOW-UP DEI CASI

	AZIONI INTRAPRESE	La situazione è
Aggiornamento 1		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 2		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 3		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 4		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 5		☐ migliorata ☐ invariata ☐ peggiorata Come:

Sicurezza in rete - Schema per la scuola

Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi

Scuola _____ Anno Scolastico _____

N°	Data	ora	Episodio *(riassunto)*	Azioni intraprese		Insegnante con cui l'alunno/a si è confidato	Firma
				Cosa?	Da chi?		

Ministero della Giustizia Dipartimento per la Giustizia Minorile

Istituto di Formazione Sardo Dipartimento per la Giustizia minorile Master in Criminologia clinica e Psicologia Giuridica Ufficio Studi, ricerche e attività internazionali

Centro Europeo di Studi di Nisida

iGloss@ 1.0 - l'ABC dei comportamenti devianti online.

L'abbecedàrio

iGloss@ 1.0 è un utile strumento di consultazione realizzato dall'Ufficio Studi, Ricerche e Attività Internazionali del Dipartimento Giustizia Minorile e dall'IFOS Master in Criminologia clinica e Psicologia Giuridica nell'ambito di un pluriennale progetto di ricerca sulle nuove forme della devianza e della criminalità online in età evolutiva.

Il nome è stato pensato facendo riferimento alla figura retorica dell'ossimoro e quindi all'abbinamento di termini in forte antitesi tra loro: da una parte la modernità con le particelle "i" (presente nei più famosi device) e "@" (la chiocciolina del mondo on line),

dall'altra la tradizione con i sostantivi "γλῶσσα" e "abbecedàrio", il libro che Pinocchio usava per imparare a leggere. Poiché è inevitabile che nel corso dei prossimi anni sarà necessario aggiornarlo, migliorarlo e arricchirlo, prevedendo successive edizioni che introdurranno nuovi termini e spiegazioni dei fenomeni, è stata prevista una numerazione delle edizioni che parte dalla versione base 1.0.

iGloss@, disponibile online in italiano e in inglese, è rivolto non solo agli operatori dei servizi sociali, sanitari e giudiziari ma anche ai giovani e ai loro genitori. E' infatti uno strumento di facile consultazione che permette di acquisire informazioni essenziali e accurate sulle condotte online illecite.

Il lavoro curato da Isabella Mastropasqua, Valeria Cadau e Luca Pisano si avvale della collaborazione di numerosi esperti nazionali e internazionali e del sostegno scientifico del WiredSafety Inc., l'organizzazione americana fondata dall'Avvocato Parry Aftab che è una tra le più importanti autorità al mondo nel settore della sicurezza digitale.

Le caratteristiche del Glossario

Il glossario si configura come una raccolta di termini specialistici sui comportamenti online a rischio. Ogni termine di "iGloss@" offre una sintetica spiegazione delle principali caratteristiche della condotta e una breve nota sulle sue proprietà socio giuridiche.

Uno degli obiettivi generali che attraversa tutta la progettualità è la tutela dei minori che più o meno consapevolmente possono configurarsi come "vittime" o "autori di reato". Per questo motivo alcune voci del glossario sono state maggiormente argomentate.

Nota:

Per quanto concerne i principali riferimenti normativi, relativi ad ogni comportamento deviante o criminale, utili per inquadrare le caratteristiche antisociali e/o anti giuridiche dell'azione compiuta e, quindi, favorire l'acquisizione di consapevolezza sulle conseguenze sociali e giudiziarie di queste specifiche trasgressioni, si rimanda alla versione integrale del glossario.

A

Auction fraud (comportamento criminale)

Trad. Let: Frode d'asta.

Accordo di vendita e/o acquisto online di merce attraverso sistemi di pagamento elettronico o tradizionale (ad esempio: vaglia online, ricariche di carte di credito prepagate, trasferimento di denaro tramite agenzie specializzate).

L'atto illecito consiste nell'istruire la vittima sulle modalità di pagamento, parziale o totale dell'importo concordato, che dopo la procedura non riceverà il bene acquistato.

Autolesionismo (comportamento deviante)

Da autolesione: il produrre deliberatamente una minorazione, temporanea o permanente sul proprio corpo1.

Pubblicare su alcuni social network immagini e/o messaggi inneggianti a suicidi o atti autolesionistici.

1 Cfr. Vocabolario della lingua italiana di Nicola Zingarelli, Edizione Zanichelli, Bologna, 2007

B

Baiting (comportamento criminale)

Trad. Let: L'aizzare cani contro belve alla catena2.

Prendere di mira utenti (users), nello specifico principianti (new users), in ambienti virtuali di gruppo (es: chat, game, forum) facendoli diventare oggetto di discussioni aggressive attraverso insulti e minacce per errori commessi dovuti all'inesperienza.

Vedi anche: FLAMING

2 Cfr. Dizionario Inglese-Italiano, G. Ragazzini, Zanichelli, Bologna, 2007

Bannare (comportamento deviante)

Deriv. Ingl: To ban, bandire, proibire, interdire.

Impedire a una persona di comunicare con altri utenti appartenenti alla stessa chat o ad un altro ambiente online protetto da password.

Vedi: EXCLUSION

C

Candy girl (comportamento deviante)

Trad. Let: Ragazza candita.

Denudarsi davanti a una webcam per poi vendere le foto in cambio di ricariche telefoniche o regali di scarso valore economico.

Vedi anche: SEXTING

Catfish (comportamento criminale)

Trad. Let: Pesce gatto.

Termine utilizzato per indicare chi assume online un'identità falsa perché appartenente a un altro utente.

Vedi: IMPERSONATION

Choking Game (comportamento criminale)

Trad. Let: Gioco asfissiante.

Trattasi di gioco che consiste nell'indurre a una persona consenziente una sensazione di forte vertigine o nel soffocarla.

Il comportamento trasgressivo è generalmente filmato e poi pubblicato in rete nei principali social network.

Click-baiting (comportamento deviante)

Trad. Let: Esche da click (click bait).

Contenuti e immagini postati sui social network, appositamente studiati per incuriosire e ottenere il maggiore numero di accessi e generare traffico. I link collegati contengono notizie di scarsa qualità e prive di informazioni rilevanti.

Vedi anche: CLICKJACKING, PUP, RICKROLLING

Clickjacking (comportamento deviante)

Trad. Let: Rapimento del clic.

Tecnica informatica fraudolenta in cui un utente è manipolato attraverso un collegamento ipertestuale nascosto che reindirizza l'accesso su un sito web d'interesse diverso da quello materialmente cliccato.

Cryptolocker ransomware (comportamento criminale)

Trad. Let: Riscatto informatico di crittografia bloccata

Sistema di crittografia dati che si diffonde via email.

Il virus scaricato visualizza una finestra pop-up sul computer delle vittime che informa che i file sono stati crittografati e non sono quindi più leggibili. Il virus fornisce alla vittima un timeline per pagare: se il bonifico non è effettuato entro la data indicata, i file crittografati saranno per sempre inaccessibili.

In alcuni casi viene chiesto di effettuare un pagamento in bitcoin, la moneta virtuale non tracciabile, per sbloccare il computer, ma il pagamento non garantisce che i file siano resi fruibili.

Cyberbashing (comportamento criminale)

Trad. Let: Maltrattamento informatico.

Specifica tipologia di cyberbullismo che consiste nel videoregistrare un'aggressione fisica nella vita reale per poi pubblicarla online.

Vedi: HAPPY SLAPPING

Cyberlaundering (comportamento criminale)

Trad. Let: Riciclaggio online di denaro sporco.

L'utilizzare conti correnti messi a disposizione da intestatari detti "prestaconto" o "money mule" che, al ricevimento delle somme di denaro, procedono al loro incasso e trasferimento in capo agli organizzatori del crimine. Gli svariati sistemi di trasferimento di somme utilizzati per il riciclaggio si coniugano con operazioni che ne consentono un'apparente copertura. Ad esempio: fatturazioni false; loan back, mediante il quale un soggetto giuridico si indebita e acquisisce liquidità, rilasciando le garanzie richieste grazie all'intervento di un'istituzione bancaria o finanziaria estera depositaria dei fondi di origine illecita. Se il debito non viene onorato, l'erogatore del finanziamento escute la garanzia e la soluzione avviene mediante l'utilizzo dei fondi di provenienza illecita; commingling, cioè la confusione di fondi illeciti con fondi leciti"3.

Cybersquatting (comportamento criminale)

Trad. Let: Occupazione abusiva di spazi virtuali.

Trattasi di atto illegale di pirateria informatica, che consiste nell'appropriarsi del nome di un dominio già esistente per poi rivenderlo ad un prezzo molto più alto4.

Vedi anche: TYPOSQUATTING, IMPERSONATION.

Cyberstalking (comportamento criminale)

Trad. Let: Molestia informatica.

Comportamento in rete offensivo e molesto particolarmente insistente e intimidatorio tale da fare temere alla vittima per la propria sicurezza fisica.

Vedi anche: HARASSMENT

D

Denigration (comportamento criminale)

Trad. Let: Denigrazione.

Attività offensiva intenzionale dell'aggressore che mira a danneggiare la reputazione e la rete amicale di un'altra persona, concretizzabile anche in una singola azione capace

di generare, con il contributo attivo non necessariamente richiesto, degli altri utenti di internet (“reclutamento involontario”), effetti a cascata non prevedibili.

Vedi anche: BAITING

Driving selfie (comportamento deviante)

Trad. Let: Autoscatto alla guida.

Trattasi di una specifica tipologia di Selfie che consiste nello scattare a se stessi una fotografia mentre si guida.

E

Exclusion (comportamento deviante)

Trad. Let: Esclusione, espulsione, estromissione.

Esclusione intenzionale di un soggetto, a opera di un aggressore, da un gruppo online (“lista di amici”), chat, post, game interattivo o da altri ambienti protetti da password.

Vedi anche: BANNARE, FLAMING

Eyeballing (comportamento deviante)

Trad. Let: Ammirare; guardare con estremo interesse.

Inoculare sostanza alcolica come vodka o whisky negli occhi come se fosse un collirio. Il comportamento trasgressivo è generalmente filmato e poi pubblicato in rete nei principali social network.

Tale pratica pericolosa originata in Francia, si è successivamente diffusa in Gran Bretagna e in altri Paesi Europei nella convinzione che l’assorbimento di sostanze alcoliche nella mucosa oculare generi lo “sballo” immediato.

Vedi anche: SELFIE, NEKNOMINATE, CHOKING GAME

F

Fake (comportamento criminale)

Trad. Let: Falso, finto, imitazione, contraffatto.

Alterare in modo significativo la propria identità online.

Esempi: fake account, fake conversation, fake status, fake login, fake email, fake chat, fake login page.

Vedi anche: IMPERSONATION

Flaming (comportamento criminale)

Trad. Let: Lite furibonda

Il battagliare verbalmente online attraverso messaggi elettronici, violenti e volgari, tra due contendenti che hanno lo stesso potere e che quindi si affrontano ad armi "pari", non necessariamente in contatto nella vita reale, per una durata temporale delimitata dall'attività online condivisa.

Vedi anche: BAITING

G

Grooming (comportamento criminale)

Trad. Let: Governatura di animali, strigliatura e/o tolettatura di animali; prendersi cura della propria persona.

Adescamento online tramite chat e social network in cui un cyber predatore individua una giovane vittima, instaura una relazione dapprima amicale poi confidenziale ed intima per poi sfruttarla ai fini sessuali. E' un lento processo interattivo attraverso il quale il cyber predatore si "prende cura" del mondo psicologico della vittima.

H

Harassment (comportamento criminale)

Trad. Let: Molestia, vessazione.

L'invio ripetuto nel tempo di messaggi insultanti e volgari attraverso l'uso del computer e/o del videotelefonino. Oltre a e-mail, sms, mms offensivi, pubblicazioni moleste su blog, forum e spyware per controllare i movimenti online della vittima, le telefonate mute rappresentano la forma di molestia più utilizzata dagli aggressori soprattutto nei confronti del sesso femminile.

Vedi anche: CYBERSTALKING

Happy slapping (comportamento criminale)

Trad. Let: Schiaffeggiamento felice.

Trattasi della produzione di una registrazione video di un'aggressione fisica nella vita reale a danno di una vittima e relativa pubblicazione online a cui aderiscono altri utenti, che pur non avendo partecipato direttamente all'accaduto, esprimono commenti, insulti e altre affermazioni diffamanti e ingiuriose. I video vengono votati e

consigliati come “preferiti” o “divertenti”.

Vedi anche: KNOCKOUT GAME, CYBERBASHING, DENIGRATION

Hentai (comportamento deviante)

Trad. Let: Anormalità, perversione.

La denominazione prende ispirazione dagli Hentai giapponesi che rappresentano scene di sesso estremo e particolarmente cruento nelle quali donne ma talvolta anche adolescenti subiscono molestie sessuali o stupri. Adulti e ragazzi possono interagire con il cartone animato e partecipare alle violenze sessuali cliccando appositi pulsanti.

Vedi anche: HIKIKOMORI

Hikikomori (comportamento deviante)

Trad. Let: Stare in disparte; isolarsi.

Gravissima forma di ritiro sociale, denominata nella società giapponese Hikikomori, che consiste nel rifiuto di uscire da casa, svolgere le normali attività quotidiane. In queste situazioni i ragazzi utilizzano internet come unico strumento per entrare in contatto con il mondo esterno.

Vedi anche: HENTAI

Hoax (comportamento deviante)

Trad. Let: Beffa; burla; imbroglio; bufala16.

Trattasi di notizie false, frutto dell’ideazione o diversamente originate come distorsioni di notizie vere o incomplete che possono degenerare in veri e propri reati nel caso in cui l'autore/i procurino per sé o per altri un ingiusto profitto a scapito delle vittime.

Vedi anche: SCAM

16 Cfr. Dizionario Inglese-Italiano Italiano-Inglese, G. Ragazzini, Zanichelli, Bologna, 2007.

I

Impersonation (comportamento criminale)

Trad. Let: Personificazione, sostituzione di persona.

Capacità di violare un account e accedere in modo non autorizzato a programmi e contenuti appartenenti alla persona intestataria dello stesso.

K

Keylogger (comportamento criminale)

Trad. Let: Parola composta da Key (chiave) e Log, che indica il file in cui vengono registrate le operazioni che l'utente compie durante il lavoro.

Software o dispositivo hardware che registra la pressione dei tasti 17 e la sequenza, allo scopo di impossessarsi di dati sensibili come ad esempio le password personali o le credenziali di un Conto Corrente.

17 Cfr. Dizionario Inglese-Italiano Italiano-Inglese, G. Ragazzini, Zanichelli, Bologna, 2007.

Knockout Game (comportamento criminale)

Trad. Let: Gioco del "mettere qualcuno KO".

Trattasi di un comportamento che prevede la videoregistrazione di un'aggressione fisica, che consiste nel colpire violentemente qualcuno in un luogo pubblico con un pugno, e la pubblicazione del filmato nei social network.

I video hanno poi lo scopo di ottenere il massimo numero di voti o commenti

Vedi anche: HAPPY SLAPPING, DENIGRATION

M

Mailbombing (comportamento criminale)

Trad. Let: Bombardamento tramite posta elettronica.

Tipologia di attacco informatico che consiste nell'invio di una quantità di messaggi numericamente rilevante, verso una stessa casella di posta elettronica. Ciò avviene tramite programmi denominati Mailbomber che causano il rallentamento o il blocco dei server di posta.

Vedi anche: SPAMMING

N

Neknominate (comportamento deviante)

Consiste nel filmarsi mentre si bevono grandi quantità di alcool in una volta sola, nel nominare qualcuno affinché emuli questo comportamento e infine nel postare online il video. La persona nominata deve a sua volta riprodurre il comportamento18.

Esistono altri tipi di nomination che non costituiscono comportamento deviante (es.

booknomination, in cui si cita una frase di un libro e si nominano altre persone affinché facciano lo stesso).

Vedi anche: STREAPNOMINATION

O

Outing And Trickery (comportamento criminale)

Trad. Let: Outing: rivelazione, venire allo scoperto.

Trichery: frode, inganno.

Comportamento che consiste nel pubblicare o condividere con terze persone le informazioni confidate dalla vittima in seguito a un periodo di amicizia in cui si è instaurato un rapporto di fiducia.

L'aggressore pubblica su un Blog o diffonde attraverso e-mail o altre applicazioni, senza alcuna autorizzazione dell'interessato, le confidenze spontanee (outing) dell'amico e le sue fotografie riservate o intime. Oppure può sollecitare l'"amico" a condividere online dei segreti o informazioni imbarazzanti su se stesso, su un compagno di classe, su un amico comune o su un docente (trickery), per poi diffonderli ad altri utenti della rete19.

Vedi anche: CYBERSTALKING

P

Pharming (comportamento criminale)

Trad. Let: Composto dalle parole phishing (raggio telematico finalizzato all'acquisizioni di dati personali) e farming (coltivazione, allevamento).

Forma di cybercrime che identifica un tentativo di phishing che può colpire più utenti simultaneamente20.

Vedi anche: PHISHING, WARM, WHALING

Phishing (comportamento criminale)

Trad. Let: Raggio telematico finalizzato all'acquisizione di dati personali21

Questo tipo di truffa consiste nell'invio di e-mail fraudolente che invitano la vittima a collegarsi tramite un login a pagine internet (che imitano la grafica di siti istituzionali o aziendali) dalle quali verranno carpiti i loro dati riservati quali le credenziali per l'accesso a conti on-line, carte di credito, sistemi di pagamento tramite piattaforme e-commerce22.

Vedi anche: SPEARPHISHING, WHALING

Pro Ana (comportamento deviante)

Trad. lett. Etimologia: composto da pro- e an(oressi)a.

Termine che indica la promozione di comportamenti a favore dell'anoressia.

In particolare siti, blog, community, etc, che esaltano l'anoressia e danno consigli per raggiungerla23.

Pro Mia (comportamento deviante)

Trad. lett. Etimologia: composto da pro- e (buli)mia.

Termine che indica la promozione di comportamenti a favore della bulimia.

In particolare siti, blog, community, etc, che esaltano la bulimia e danno consigli per raggiungerla24

PUP - potentially unwanted program - (comportamento deviante)

Trad. Let: Programma potenzialmente non desiderato

Trattasi di programma potenzialmente indesiderato che può essere involontariamente scaricato durante il download di un software 25 . Si tratta quindi dell'inserimento, nel file d'installazione di un programma, di componenti superflui assolutamente non necessari per il funzionamento dell'applicazione alla quale si è interessati. Non si tratta quindi di un malware, creato con l'intento di danneggiare il computer o rubare informazioni personali, ma di un programma finalizzato a istallare senza consenso altri programmi indesiderati (ad esempio "adware" o "toolbar")26.

R

Rickrolling (comportamento deviante)

Trad. Let: Rickrolling: distorsione, dannoso.

Trattasi di portare con l'inganno una persona a cliccare su un collegamento ipertestuale che porta invece a qualcosa di diverso da quanto sostenuto inizialmente27.

Un esempio celebre di Rickrolling è il caso della canzone "Never Gonna Give You Up" di Rick Astley a cui milioni di persone sono state reindirizzate cliccando link che fornivano informazioni su differenti aree tematiche.

Vedi anche: CLICKJACKING, PUP, CLICK BAITING

Romance Scam (comportamento deviante)

Trad. lett: Frode romantica.

Trattasi di una frode che prevede l'instaurazione di un contatto, attraverso chat, siti per single e piattaforme simili, con potenziali vittime che, illudendosi di avere iniziato una storia d'amore, sono disponibili a prestare o regalare importanti quantità di denaro.

Vedi: SCAM

S

Scam (comportamento criminale)

Trad. lett: Truffa, imbroglio, macchinazione.

Trattasi di modo illegale per ottenere denaro.

Questo genere di truffa può riguardare le seguenti aree:

1. trasferimento di importanti somme di denaro: in questo caso il truffatore chiede alla vittima un deposito cauzionale e/o il numero di conto corrente bancario e offre una ricompensa per il denaro recuperato;

2. vincita alla lotteria che può essere ritirata versando però una tassa;

3. messaggi sentimentali e successive richieste di aiuto economico per acquistare il biglietto aereo, curare una grave malattia o sostenere le spese burocratiche necessarie per acquisire i documenti per sposarsi;

4. richieste di matrimonio finalizzate ad ottenere la cittadinanza.

Sexting (comportamento deviante)

Trad. lett: Composto dalle parole sex (sesso) e texting (inviare SMS).

Atto di inviare fotografie e/o messaggi di testo sessualmente espliciti. Solitamente tale comportamento viene posto in essere attraverso telefoni cellulare, ma anche tramite mezzi informatici differenti 28

Vedi anche: SEXTORTION

Sextortion Scams (comportamento criminale)

Trad. lett: Deriva dall'unione delle parole inglesi "sex" (sesso) ed "extortion"

(estorsione).

Trattasi di truffa perpetrata ai danni di utenti internet ai quali, con l'illusione di un flirt o una storia sentimentale, sono estorte immagini erotiche usate poi come strumento di ricatto.

Vedi anche: SEXTING

Smishing And Vishing (comportamento criminale)

Smishing

Trad. lett: Truffa con sms (da SMS + phishing).

Trattasi di truffa riconducibile al phishing, effettuata attraverso gli SMS. La vittima riceve SMS da un falso mittente che ha il fine ultimo di ottenere in modo fraudolento i suoi dati d'accesso ai servizi online (banca, carta di credito, etc).

Vishing

Trad. lett: Truffa a mezzo voce (da Voice + phishing).

Trattasi di truffa riconducibile al phishing, perpetuata attraverso una chiamata telefonica.

Vedi anche: SCAM

Sniffing (comportamento criminale)

Trad. lett: Sniffare, annusare, fiutare.

Definisce l'attività di intercettazione dei dati che transitano in una rete telematica30. Tale attività può avere finalità legittime (risolvere problemi tecnici o evitare intrusioni da parte di terzi) oppure illecite (ottenere password, codici per l'home banking, dati sensibili, ecc). 31

Vedi anche: SCAM

Spamming (comportamento criminale)

Trad. Let: Inondazione (di caselle di altri utenti) con messaggi indesiderati.

Trattasi dell'invio di mail indesiderate (generalmente di tipo commerciale/pubblicitario) a un gran numero di destinatari che non hanno prestato il proprio consenso ("opt in") a questa ricezione, creando di conseguenza l'intasamento della casella di posta elettronica.

Talvolta può essere utilizzato anche il termine Junk-Mail (Trad. Let: Messaggio inutile).

Vedi anche: PHISHING, SPEARPHISHING, SPIM, WHALING

Spearphishing (comportamento criminale)

Trad. Let: Spear: lancia, arpione + phishing.

Trattasi di campagne di truffe mirate. Dopo avere osservato online gli interessi delle vittime (grazie alle informazioni che pubblicano nei social network), i truffatori inviano email non più generiche, come nel phishing classico, ma personalizzate, rendendo con i dettagli in esse contenute più credibile il messaggio.

Vedi anche: PHISHING, SPIM, TABNABBING, WHALING

Spim (comportamento criminale)

Trad. let: Acronimo di Messaging Spam.

Nelle applicazioni di Instant Messaging, indica lo spamming che generalmente, invita l'utente a collegarsi a un sito web.

Vedi anche: PHISHING, SPEARPHISHING, SPAMMING, WHALING

Spoofing (comportamento criminale)

Trad. lett: Presa in giro; farsi beffa di qualcuno.

Trattasi di comportamento messo in atto dallo spoofer.

Spoofer è colui che falsifica dati e protocolli con l'intento di apparire un'altra persona o di accedere ad aree riservate.

Le tecniche di spoofing sono diverse, le più note e adoperate sono32:

Spoofing dell'IP (falsificazione di pacchetti IP al fine di nasconderne la presenza) 33

Spoofing del DSN

Spoofing dell'ARP

Web Spoofing

SMS Spoofing

Mail Spoofing

Vedi anche: IMPERSONATION, CATFISH, TABNABBING

Streapnomination (comportamento criminale)

Trad. Let: Nomination dello streep tease

Si indica il comportamento di una persona che, nominata da un amico online, si spoglia in un luogo pubblico e affollato al fine di produrre un video che sarà poi diffuso nei principali social network.

Vedi anche: NEKNOMINATION

T

Tabnabbing (comportamento criminale)

Trad. lett: Catturare la scheda di un browser.

Trattasi di truffa online che prende di mira le schede aperte (TAB) nel browser sostituendone il contenuto con una pagina identica, creata appositamente per richiedere all'utente a inserire i propri dati personali che saranno poi copiati. È una forma più raffinata di phishing.

Vedi anche: IMPERSONATION, CATFISH

Thinspiration (comportamento deviante)

Trad.lett: Ispirazione al dimagrimento.

Termine che indica la promozione di comportamenti a favore dell'anoressia attraverso la pubblicazione di fotografie che rappresentano persone esageratamente magre.

Vedi: PRO ANA

Troll (comportamento deviante)

Trad. lett: Sgobbone, secchione.

Trattasi di persona che scrive un commento provocatorio a un post o una frase (negativamente) mirata, al fine di generare una risposta scontrosa. Il termine è utilizzato nei news-groop, nei forum, nei blog e nelle mailing list.

Vedi anche: DENIGRATION

Typosquatting (comportamento criminale)

Trad. lett: Occupazione abusiva di spazi virtuali tramite errore di battitura.

Trattasi di una forma illegale che consiste nel dirigere utenti che per sbaglio commettono un errore nella battitura dell'indirizzo URL, verso siti internet dal nome molto simile.

Spesso questa è una strategia utilizzata per diffondere malware.

Vedi anche: CYBERSQUATTING, IMPERSONATION.

V

Violazione dell'account (comportamento criminale)

Trattasi di fenomeno complesso che comprende in particolare:

- violazione dell'account di piattaforma di commercio elettronico (o di bacheche di annunci vendita) al fine di porre fittiziamente in vendita su internet, avvalendosi di un'identità non corrispondente a quella reale, beni di varia natura con l'intento di non procedere poi all'invio dell'oggetto in questione e impossessarsi della somma di denaro35;

- violazione/acquisizione indebita dell'account per accedere ai social network36.

Whaling (comportamento criminale)

Trad.lett: Caccia alla balena.

Tipologia di attacco informatico che prevede l'invio di e-mail personalizzate, aumentando in tal modo la credibilità del contenuto del messaggio, al fine di truffare persone con un alto profilo professionale (es. manager).

Vedi anche: PHISHING, SPEARPHISHING, SPIM, TABNABBING

Scheda di approfondimento:

I PRINCIPALI REATI PROCEDIBILI D'UFFICIO

Gli insegnanti, in quanto incaricati di pubblico servizio, hanno obbligo di denuncia qualora vengano a conoscenza di reati perseguibili d'ufficio. A questa categoria appartengono i seguenti reati:

Delitti "sessuali" (art. 609 bis e seguenti c.p.)

1. Violenza sessuale commessa nei confronti di minore di anni 18;

2. Violenza commessa dal genitore (anche adottivo) o dal di lui convivente, dal tutore o da persona alla quale il minore sia affidato per ragioni di cura, di

educazione, di istruzione, di vigilanza o di custodia;

3. Violenza sessuale di gruppo;

4. Corruzione di minorenne (chi compie atti sessuali in presenza di un minore di 14 anni al fine di farlo assistere; chi fa assistere l'infra-quattordicenne ad atti sessuali o mostra materiale pornografico al fine di indurlo a compiere o subire atti sessuali);

5. Adescamento di minorenni (chi allo scopo di commettere reati di prostituzione minorile, pornografia minorile, detenzione di materiale pornografico, violenza sessuale, ...adesca un minore infra-sedicenne).

Prostituzione minorile* (600 bis)

Punisce chi recluta o induce alla prostituzione un minore di 18; favorisce, sfrutta, gestisce, ...la prostituzione di un minore di 18 anni; chi compie atti sessuali con un minore tra i 14 e i 18 anni in cambio di corrispettivo di denaro o altra utilità, anche solo promessi.

Pornografia minorile* (art. 600 ter) e Detenzione di materiale pedopornografico* (art. 600 quater c.p.)

Il presenti reati puniscono: chi utilizzando minori di anni diciotto realizza esibizioni o spettacoli pornografici ovvero produce materiale pornografico; chi recluta, induce minori di anni diciotto a partecipare a tali esibizioni o ne trae profitto; chi anche con il mezzo telematico, distribuisce, divulga, pubblicizza notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori di 18 anni; chi assiste a esibizioni o spettacoli pornografici in cui sono coinvolti minori di 18 anni; chi consapevolmente si procura, detiene, offre o cede ad altri, anche a titolo gratuito il materiale pornografico realizzato utilizzando minori di anni diciotto.

Minaccia* (art. 612 c.p)

Se qualcuno viene minacciato in modo grave (p.e. di morte) o con armi.

Lesione personale* (art. 582 c.p.)

Punisce chi procura lesione da cui deriva una malattia nel corpo o nella mente con prognosi superiore a 20 giorni o con circostanze aggravanti.

Stalking - atti persecutori* (art 612 –bis)

Chiunque, con condotte reiterate, minaccia o molesta un minore o una persona con disabilità (art.3 della legge 104/92) in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l’incolumità propria o

di un prossimo congiunto o di persona al medesimo legata da relazione affettiva, ovvero da costringere lo stesso ad alterare le proprie abitudini di vita.

Istigazione al suicidio* (art. 580 c.p.)

Chiunque determina altri al suicidio o rafforza l'altrui proposito di suicidio, ovvero ne agevola in qualsiasi modo l'esecuzione, è punito, se il suicidio avviene, con la reclusione da cinque a dodici anni. Se il suicidio non avviene, è punito con la reclusione da uno a cinque anni, sempre che dal tentativo di suicidio derivi una lesione personale grave o gravissima.

Estorsione* (art. 629 c.p.)

Punisce chi mediante violenza o minaccia costringe una persona a fare o omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno.

Violenza privata* (art. 610 c.p.)

Se una persona viene costretta con violenza o minaccia a fare, tollerare o omettere qualcosa (ad es. dover andare con qualcuno, ovvero non poter uscire ecc).

Sostituzione di persona* (art. 494 c.p.)

Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici.

Delitti contro l'assistenza famigliare (artt. 570 e seg. c.p.)

1. Violazione degli obblighi di assistenza famigliare se commessi nei confronti di minori

2. Abuso di mezzi di correzione o di disciplina;

3. Maltrattamenti in famiglia o verso i fanciulli.

*REATI ON-LINE: la maggior parte dei reati sopra citati possono essere commessi anche on-line ovvero attraverso l'utilizzo di dispositivi connessi alla rete. Questa circostanza, che spesso rende più difficile l'individuazione del reato e più facile la sua attuazione da parte dei minori, può costituire in alcuni casi una aggravante del reato stesso.

Non ci sono tuttavia reati specifici che descrivono questi comportamenti on-line e si deve quindi fare riferimento ai reati sopra elencati. Ad esempio i comportamenti come

il Cyberbullismo e il Sexting vanno valutati caso per caso in quanto possono includere uno o più dei reati perseguibili d'ufficio sopra elencati.

Il nostro piano d'azioni

Sulla base delle Linee guida per l'uso positivo delle tecnologie digitali e della prevenzione dei rischi nelle scuole (MI - Generazioni Connesse Safer Internet Centre), vengono assunti i seguenti punti quali indicatori di co-costruzione tra scuola-famiglia-servizi territoriali, al fine di creare un modello composito e lineare di azioni condivise:

- coinvolgimento di tutti gli attori della scuola: studenti e studentesse, docenti, genitori e personale ATA per la realizzazione di un'autentica comunità educante;
- alleanza educativa tra scuola e famiglia;
- interventi educativi ed azioni di supporto, quale prevenzione per eventuali comportamenti a rischio;
- misure preventive specifiche di tutela anche con l'ausilio di attori territoriali, come le Forze dell'Ordine e ASL;
- promozione dell'educazione al rispetto;
- sviluppo del pensiero critico;
- promozione dell'Educazione Civica Digitale.