SIC (Safer Internet Center) – Generazioni connesse

Policy di E-Safety I.C. "E.Fermi" Reggio Emilia

INDICE RAGIONATO
E-Safety Policy

1. Introduzione

- Scopo della Policy.
- Ruoli e Responsabilità (*che cosa ci si aspetta da tutti gli attori della Comunità Scolastica*).
- Condivisione e comunicazione della Policy all'intera comunità scolastica.
- Gestione delle infrazioni alla Policy.
- Monitoraggio dell'implementazione della Policy e suo aggiornamento.
- Integrazione della Policy con Regolamenti esistenti.

2. Formazione e Curricolo

- Curricolo sulle competenze digitali per gli studenti.
- Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica.
- Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
- Sensibilizzazione delle famiglie.

3. Gestione dell'infrastruttura e della strumentazione ICT della scuola.

- Accesso ad internet: filtri, antivirus e sulla navigazione.
- Gestione accessi (password, backup, ecc.).
- E-mail.
- Blog e sito web della scuola
- Social network.
- Protezione dei dati personali.

4. Strumentazione personale

- Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc..
- Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc..
- Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc.

5. Prevenzione, rilevazione e gestione dei casi

Prevenzione

- Rischi
- Azioni

Rilevazione

- Che cosa segnalare
- Come segnalare: quali strumenti e a chi.
- Come gestire le segnalazioni.

Gestione dei casi

- Definizione delle azioni da intraprendere a seconda della specifica del caso.

Annessi (da prodursi a cura della scuola)

1. Procedure operative per la gestione delle infrazioni alla Policy.
2. Procedure operative per la protezione dei dati personali.
3. Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni.
4. Procedure operative per la gestione dei casi.
5. Protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi.

1. Introduzione

1.1 Scopo della Policy

La E Safety Policy di questo istituto ha lo scopo di descrivere le norme comportamentali e le procedure per l'utilizzo delle ICT nell'Istituto Comprensivo "E. Fermi" di Reggio Emilia, le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse a un uso non consapevole delle tecnologie digitali.
Il nostro istituto ha già prodotto, nel mese di ottobre 2016, un Piano d'Azione che individua il percorso e le risorse necessarie per elaborare e, nel tempo, implementare una Policy di E- Safety, individuando due obiettivi principali:

1) adottare le misure atte a facilitare e a promuovere l'uso delle ICT nella didattica e negli ambienti scolastici;
2) stabilire le misure di prevenzione e di gestione di situazioni problematiche relative all'uso delle tecnologie digitali.

Grazie a un percorso guidato e al materiale di supporto messo a disposizione sul sito del progetto www.generazioniconnesse.it, si definiscono qui le misure che l'Istituto intende adottare:

a) per la promozione dell'utilizzo delle ICT nella didattica;
b) per la prevenzione, ovvero le azioni finalizzate alla prevenzione di fenomeni legati ai rischi delle tecnologie digitali;
c) per la segnalazione dei casi, ovvero le disposizioni semplici su come segnalare i casi nella scuola;

d) per la gestione dei casi, ovvero le misure che la scuola intende attivare a supporto delle famiglie e degli studenti che sono stati vittime o spettatori attivi e/o passivi di quanto avvenuto.

Occorre, inoltre, premettere che
a) il progetto "Generazioni connesse" è stato inserito nel Piano Triennale dell'Offerta Formativa d'Istituto e le azioni preventivate nel Piano d'Azione della nostra scuola si propongono di realizzarlo e di diffonderlo, in accordo con le priorità di potenziamento delle competenze relazionali, di cittadinanza e convivenza interculturale individuate per i Piani di Miglioramento.
b) le attività di sensibilizzazione all'utilizzo delle tecnologie digitali nella didattica costituiscono un tema centrale per l'attuazione del Piano Nazionale Scuola Digitale e la scuola promuoverà tutte le azioni necessarie per la prevenzione e la gestione dei casi di scorretto utilizzo delle tecnologie in promuovendone un uso quotidiano e consapevole.

1.2. Ruoli e responsabilità

Nell'ambito di questa policy sono individuati i seguenti ruoli e le principali responsabilità correlate:
1) Dirigente scolastico:

- garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- invitare i propri docenti a una formazione di base sulle Tecnologie dell'Informazione e della Comunicazione (TIC) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse;
- favorire l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on line;

2) Animatore digitale, come da PNSD:

- creare soluzioni innovative - individuare soluzioni metodologiche e tecnologiche sostenibili da diffondere all'interno degli ambienti della scuola (es. uso di particolari strumenti per la didattica di cui la scuola si è dotata; adozione di metodologie comuni; informazione su innovazioni esistenti in altre scuole; laboratorio di coding per tutti gli studenti), coerenti con l'analisi dei fabbisogni della scuola stessa, anche in sinergia con attività di assistenza tecnica condotta da altre figure.

3) Direttore dei Servizi Generali e Amministrativi:

- assicurare, nei limiti delle risorse finanziarie disponibili (e tenendo presenti proposte di finanziamento e promozione di bandi dedicati all'acquisto di nuovi strumenti digitali), gli interventi di manutenzione richiesti da cattivo funzionamento e/o danneggiamento della dotazione tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate;
- facilitare la trasmissione di comunicazioni relative alle tecnologie digitali tra le varie componenti della scuola (Dirigente scolastico, Animatore digitale, docenti e famiglie degli alunni);
- curare la registrazione dei disservizi e delle problematiche relative alla rete e all'uso del digitale segnalate dai docenti, provvedendo all'intervento del personale tecnico di assistenza.

4) Docenti:

- curare personalmente la propria formazione/aggiornamento sull'utilizzo del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in Internet e dell'immagine degli altri: lotta al cyberbullismo);
- inserire tematiche legate al corretto uso delle TIC e delle possibili conseguenze derivanti dalla violazione delle norme stabilite nelle unità di apprendimento delle singole discipline;
- sviluppare le competenze digitali degli alunni (così come previsto dalla Life Long Learning) e fare così in modo che conoscano e seguano le norme di sicurezza nell'utilizzo del web e utilizzino correttamente le tecnologie digitali sia a scuola sia nelle attività didattiche extracurricolari;
- segnalare prontamente alle famiglie eventuali problematiche emerse in classe nell'utilizzo del digitale e stabilire comuni linee di intervento educativo per affrontarle;
- segnalare al dirigente scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazioni.

5) Allievi:

- ascoltare e seguire le indicazioni fornite dai docenti per un uso corretto e responsabile delle tecnologie digitali, attuando le regole di e-safety per evitare situazioni di rischio;

6) Genitori:

- contribuire, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- partecipare a momenti di informazione e formazione promossi dalla scuola, anche con i propri figli, per condividere preoccupazioni, soluzioni, conoscenza dei rischi e delle possibilità positive legate alle TIC.
- agire in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite.

1.3. Condivisione e comunicazione della Policy all'intera comunità scolastica.

a) Condivisione e comunicazione della Policy agli alunni:

All'inizio dell'anno, in occasione dell'illustrazione del regolamento d'istituto agli alunni da parte dei docenti, verrà presentata questa policy, insieme ai regolamenti correlati.
Nel corso dell'anno saranno dedicate da ciascun docente alcune lezioni alle buone pratiche per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta al cyberbullismo e con l'aiuto e il supporto dei materiali e delle opportunità fornite da Generazioni Connesse e da esperti esterni.

b) Condivisione e comunicazione della Policy al personale:

La Policy adottata dalla scuola in materia di sicurezza digitale sarà presentata agli organi collegiali (collegio docenti, riunioni di dipartimento, consigli di classe) e resa nota all'intera comunità scolastica tramite pubblicazione del presente documento sul sito web della scuola.
Il personale della scuola riceverà un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso materiali resi disponibili anche sul sito web della scuola.

c) Condivisione e comunicazione della Policy ai genitori:
Le famiglie saranno informate in merito alla linea di condotta adottata dalla scuola per un uso sicuro e responsabile delle tecnologie digitali e di internet tramite i rappresentanti dei genitori e attraverso la condivisione del presente documento e di materiali informativi specifici sul sito web della scuola.
Al fine di sensibilizzare le famiglie sui temi dell'uso delle TIC saranno organizzati dalla scuola incontri informativi, durante i quali si farà riferimento alla presente policy.

1.4. Gestione delle infrazioni alla Policy.

In relazione a quanto specificato in questa policy (e in modo particolare nella definizione dei ruoli del capitolo 1.2 e nelle regole descritte nei capitoli 3, 4 e 5), le infrazioni saranno gestite in modo graduale rispetto alla gravità dell'infrazione e, nel caso degli alunni, anche alla loro età.
1) Infrazioni degli alunni.

È bene che i docenti introducano, preventivamente, attività laboratoriali miranti a sviluppare nei loro alunni una sempre maggiore consapevolezza dei rischi legati a un uso imprudente e improprio del web e che forniscano loro, ogniqualvolta avvenga un'infrazione alle regole stabilite, gli strumenti per affrontare le conseguenze dei loro errori.
I provvedimenti disciplinari da adottare da parte del consiglio di classe nei confronti dell'alunno che ha commesso un'infrazione alla policy (in proporzione sia all'età dello studente sia alla gravità dell'infrazione commessa) saranno i seguenti:

- richiamo verbale al singolo alunno e all'intera classe, anche tramite lavoro per gruppi;
- sanzioni estemporanee commisurate alla gravità della violazione commessa;
- nota informativa sul diario ai genitori;
- convocazione dei genitori per un colloquio con l'insegnante;
- convocazione dei genitori per un colloquio con il dirigente scolastico.

2) Infrazioni del personale scolastico.

Le infrazioni alla policy da parte del personale scolastico possono riguardare sia la mancata osservanza delle regole qui descritte sulla gestione della strumentazione, sia la mancata sorveglianza e pronto intervento nel caso di infrazione da parte degli alunni.
Nel primo caso la gravità si valuta sull'esposizione al rischio procurata agli alunni, nel secondo caso sul danno per la non tempestiva attivazione delle azioni qui indicate.

Le infrazioni riscontrate saranno segnalate al dirigente scolastico che, valutata la gravità, potrà provvedere con una ammonizione informale a voce o una ammonizione scritta.

1.5. Monitoraggio dell'implementazione della Policy e suo aggiornamento.

Il monitoraggio dell'implementazione della Policy avverrà:

- alla fine di ogni anno scolastico, contestualmente alla revisione o alla nuova redazione del Rapporto di Autovalutazione, e sulla base dei casi problematici riscontrati e della loro gestione;
- all'inizio di ogni anno scolastico, contestualmente alla revisione del PTOF, a cura del Dirigente scolastico, dell'Animatore Digitale e dei collaboratori del Dirigente, anche attraverso la somministrazione ad alunni e docenti di questionari atti a verificare l'insorgenza di nuove necessità, e alla revisione delle tecnologie esistenti.

1.6. Integrazione della Policy con Regolamenti esistenti.

Il presente documento si integra pienamente con obiettivi e contenuti dei seguenti documenti, che specificano il contesto di attuazione delle politiche dell'Istituto Comprensivo per un uso consapevole ed efficace del digitale nella didattica:

- PTOF, incluso il piano per l'attuazione del PNSD;
- Regolamento interno d'istituto;
- Regolamento per l'utilizzo dei laboratori di informatica.

2. Formazione e Curricolo

2.1. Curricolo sulle competenze digitali per gli studenti.

In quest'ambito si seguono le indicazioni contenute nel PNSD, in cui si individuano alcuni framework di riferimento per la definizione e lo sviluppo delle competenze digitali, tra cui il framework DIGCOMP, che prevede 21 competenze, di cui alcune specifiche nell'area della sicurezza. Nella definizione del curricolo si farà anche riferimento al modello sviluppato dal team di lavoro del prof. Vincenzo Bonomolo per il Digital Competence Assessment.

2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica

Le attività di formazione si svolgeranno su due livelli:

- formazione istituzionale, organizzata dal Miur secondo il PNSD, attraverso gli snodi formativi;
- formazione specifica di Istituto, legata alle esigenza formative rilevate ad inizio d'anno a cura dell'Animatore Digitale.

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

Al fine di promuovere la condivisione di buone pratiche per un uso consapevole e sicuro delle TIC, e di prevenire e contrastare "ogni forma di discriminazione e del bullismo, anche informatico" (Legge 107/2015, art. 1, c. 7, l), il nostro Istituto ha aderito, quest'anno, al progetto Generazioni Connesse (SIC Italy II), coordinato dal MIUR, in partenariato con il Ministero dell'Interno-Polizia Postale e delle Comunicazioni e con altre importanti associazioni per la tutela dei diritti dei minori, come Children Italia e Telefono Azzurro.

2.4. Sensibilizzazione delle famiglie

Da ormai 5 anni il nostro istituto organizza incontri aperti alle famiglie e agli studenti, in autonomia o in collaborazione con Enti locali e Agenzie formative, per sensibilizzare docenti,

alunni e genitori sui temi della sicurezza online. Si tratta di appuntamenti ormai tradizionali la cui programmazione continuerà anche nei prossimi anni, che offrono occasioni di confronto e discussione sui rischi rappresentati da cellulari, smartphone e chat line senza un'adeguata formazione che prevenga l'uso inappropriato di tali dispositivi. Sul sito scolastico saranno resi accessibili i materiali, tra cui guide in formato pdf e video dedicati alle famiglie e ai ragazzi, presenti nella bacheca virtuale del sito di "Generazioni connesse".

La scuola darà inoltre ampia diffusione, tramite pubblicazione sul sito, del presente documento di policy per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e favorire un'attiva collaborazione tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi a un uso inappropriato del digitale.

3. Gestione dell'infrastruttura e della strumentazione TIC della scuola

3.1. Accesso a internet: filtri, antivirus e sulla navigazione

L'accesso a internet è possibile, nei tre plessi della scuola primaria ("V. Agosti", "San G. Bosco" e "Mons.Canossini" e nella scuola secondaria di primo grado, "Enrico Fermi", in tutte le aule (compreso il Laboratorio di Scienze nel seminterrato del plesso "E. Fermi") dotate di Lavagna Interattiva Multimediale con relativo computer portatile. Nel plesso della secondaria "E. Fermi" un'aula al terzo piano ospita la cl@sse 2.0 e l'accesso a internet è possibile anche dal laboratorio di informatica, dall'Aula Magna e da un ambiente con postazioni PC a disposizione del personale.
Nei laboratori di informatica e nelle aule sono attivi filtri per la navigazione sicura, tramite gestione di blacklist, ed è prevista l'attivazione di software per la gestione e il controllo delle postazioni.
Le impostazioni sono definite e manutenute dall'Animatore Digitale ed è in carico a ciascun docente la segnalazione di malfunzionamenti e disservizi.
I docenti hanno piena autonomia nel collegamento ai siti web nelle postazioni a loro riservate.
Nota: I plessi dell'Istituto sono tutti sono cablati, quindi l'accesso a internet via tablet o comunque con postazioni mobili, da parte dei docenti e del personale, è possibile ovunque nelle scuole, previa autorizzazione e registrazione dei dispositivi da parte dell'Amministratore.

3.2. Gestione accessi (password, backup, ecc.).

Nei computer presenti nelle aule e nei laboratori sono previsti tre profili di accesso con password relative:

- amministratore
- docente
- alunno

È possibile effettuare installazioni e aggiornamenti di software solo tramite la password di amministratore, a disposizione del personale di assistenza tecnica e dell'Animatore Digitale.
Non è previsto un backup automatico su server e non è al momento attiva una politica di backup.

3.3. E-mail.

L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. Le credenziali sono in possesso del personale amministrativo.
I docenti utilizzano per scopi didattici il proprio account su dominio edu.it; la posta elettronica è

protetta da antivirus e da antispam.

3.4. Blog e sito web della scuola.

La scuola ha un sito web. Tutti i contenuti del settore didattico sono pubblicati direttamente sotto la supervisione dell'Animatore digitale, che ne valuta con il Dirigente scolastico la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc.
Esiste dall'a.s.2016-17 anche un blog della scuola nato dal progetto di potenziamento di italiano (giornalismo), che viene aggiornato a seconda delle progettualità annuali.
I contributi degli alunni sono pubblicati dai docenti che ne discriminano criteri, pertinenza e appropriatezza allo strumento di diffusione.

3.5. Social network

Attualmente nella didattica non si utilizzano social network, neanche da parte dell'istituzione scolastica e il personale scolastico non è autorizzato a utilizzarli per nome e per conto della stessa. Si potrà fare eccezione in caso di partecipazione ad iniziative specifiche (come la diffusione di un evento e la sua pubblicazione sulla pagina di Facebook) previa richiesta di autorizzazione e supervisione del Dirigente.

3.6. Protezione dei dati personali.

Il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Tutto il personale incaricato riceve poi istruzioni particolareggiate applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi.
Viene inoltre fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni, eccedente i trattamenti istituzionali obbligatori.

4. Strumentazione personale

4.1. Per gli studenti: gestione degli strumenti personali – cellulari, tablet, ecc.

Come espresso dal Regolamento di Istituto, gli alunni si impegnano a tenere spenti e custoditi nello zaino i telefoni cellulari. In caso di urgenza per comunicazioni tra gli alunni e le famiglie, su autorizzazione dei docenti e sotto il diretto controllo dei collaboratori scolastici, gli alunni potranno comunicare con le famiglie tramite gli apparecchi telefonici della scuola. Non è consentito l'uso di dispositivi personali.

4.2. Per i docenti: gestione degli strumenti personali – cellulari, tablet, ecc.

Durante le ore di lezione è consentito ai docenti l'uso di dispositivi elettronici personali, come il tablet, unicamente a scopo didattico e a integrazione dei dispositivi scolastici disponibili (il computer di classe), in special modo per l'utilizzo del registro elettronico. Durante il restante orario di servizio, l'uso del cellulare è consentito solo per comunicazioni personali che rivestano carattere di urgenza, mentre l'uso di altri dispositivi elettronici personali è permesso per attività funzionali all'insegnamento.

4.3. Per il personale della scuola: gestione degli strumenti personali – cellulari, tablet, ecc.

Durante l'orario di servizio al restante personale scolastico l'uso del cellulare è consentito per comunicazioni personali urgenti.
L'uso di altri dispositivi elettronici personali è permesso solo per attività funzionali al servizio, e preventivamente autorizzato.

5. Prevenzione, rilevazione e gestione dei casi

5.1. Prevenzione 5.1.1. Rischi

Al personale che opera nella scuola, e in modo particolare agli insegnanti, viene oggi offerta la possibilità di essere promotori e garanti della costruzione dialogica di un percorso formativo partecipato, e per il loro ruolo diventano spesso inevitabilmente confidenti degli alunni e delle loro esperienze. Proprio per questo, gli insegnanti sono avamposto privilegiato per l'osservazione delle problematiche e dei rischi che bambini e adolescenti possono trovarsi ad affrontare ogni giorno. Basti pensare all'elevato numero di casi di bullismo e di cyberbullismo che i docenti rilevano durante il loro insegnamento quotidiano.

La prima responsabilità degli insegnanti consiste, dunque, nell'imparare a riconoscere i rischi più comuni che i ragazzi possono correre navigando in rete, per potere poi intervenire adeguatamente. Tra questi, un'attenzione specifica andrà prestata ai fenomeni di bullismo/cyberbullismo – una forma di prepotenza virtuale attuata attraverso l'uso di internet e delle tecnologie digitali –; sexting - pratica di inviare o postare messaggi di testo e immagini a sfondo sessuale, come foto di nudo o semi-nudo, via cellulare o tramite Internet – e adescamento o grooming – una tecnica di manipolazione psicologica, che gli adulti potenziali abusanti utilizzano online, per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata (Glossario di "Generazioni connesse"). L'adulto tenta di avvicinare un/a bambino/a o adolescente per scopi sessuali, conquistandone la fiducia attraverso l'utilizzo della rete Internet. In un primo tempo, spesso mentendo sulla propria identità e sulla propria età, mostra particolare interesse nei confronti del/la bambino/a o dell'adolescente e solo in un secondo tempo, cerca di entrare sempre più nell'intimità fino a introdurre argomenti attinenti la sfera sessuale.

I rischi che i ragazzi possono correre a scuola nell'utilizzo di dispositivi digitali possono derivare principalmente da un uso non corretto del telefono cellulare o di altri dispositivi come lo smartphone o il tablet. Sebbene, infatti, l'uso del cellulare e dello smartphone non sia consentito dal Regolamento dell'Istituto, alcuni bambini della scuola primaria e quasi tutti i ragazzi della secondaria vengono a scuola con uno di questi dispositivi che dovrebbero tenere spenti durante le lezioni. Accade tuttavia che, in orario scolastico, alcuni studenti, eludendo la sorveglianza del personale della scuola, accendano e usino il cellulare o lo smartphone, non solo per comunicare con i propri genitori, ma anche per navigare su internet, andando su siti non adatti e inviando materiali riservati (foto, video e altro). Così facendo, gli studenti possono incorrere anche a scuola nei rischi che abbiamo menzionato sopra, entrando in contatto e persino in confidenza con sconosciuti, fino a ricevere messaggi molesti e adescamenti.

5.1.2. Azioni

L'obiettivo che l'insegnante deve proporsi, dopo avere riconosciuto il pericolo, è agire di conseguenza, con azioni di contrasto efficaci e mirate, rispetto ai rischi sopra elencati.

Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli studenti in orario scolastico, vi sono le seguenti:

- diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web, condividendo materiali messi a disposizione sul sito del progetto "Generazioni connesse";

- richiedere autorizzazione esplicita da parte dei genitori all'utilizzo dei dati personali degli alunni (es. liberatoria per la pubblicazione di foto, immagini, video relativi al proprio/a figlio/a per la partecipazione a progetti didattici e altro);

- far rispettare il divieto di utilizzo di dispositivi digitali propri, quali cellulare e smartphone, agli studenti in orario scolastico. Le dovute eccezioni (uso del cellulare per comunicazioni alunno-famiglia in occasione di uscite didattiche) andranno espressamente regolamentate e dovranno comunque avvenire sotto la supervisione diretta di un docente responsabile;

- dotare i dispositivi della scuola di filtri che impediscano l'accesso a siti web non adatti ai minori (black list).

Le azioni utili a impedire un utilizzo incauto, scorretto o criminoso degli strumenti digitali – materiali inviati, scaricati, ricevuti o condivisi – su dispositivi digitali in uso a scuola (principalmente pc) sono:

- bloccare l'accesso a un sito o a un insieme di pagine impedendone la consultazione;
- controllare periodicamente i siti visitati dagli alunni;
- utilizzare un software in grado di intercettare le richieste di collegamento e di respingere quelle non conformi alle regole stabilite dall'amministratore;
- affidare a un gruppo di docenti scelto le regole di filtraggio.

5.2. Rilevazione 5.2.1. Che cosa segnalare

La diffusione capillare dei social network tra i bambini e ancor più tra gli adolescenti, li espone sempre più spesso al rischio di inviare o condividere, senza alcuna protezione, materiali personali o riservati. Discutendo in classe dei rischi del web e confrontandosi sulle esperienze personali o dei propri coetanei, emergono spesso fatti che "allarmano" l'insegnante. Il docente ha la possibilità, anzi il dovere, di intervenire sui dispositivi digitali in uso a scuola, mentre non può intervenire direttamente sui telefoni cellulari dei bambini senza un'esplicita autorizzazione delle famiglie.

Tra i contenuti rilevati che devono essere opportunamente segnalati vi sono:

- dati sensibili o riservati (foto, immagini, video personali, informazioni private proprie o di amici; l'indirizzo di casa o il telefono, ecc.);

- contenuti che possano considerarsi in qualche modo lesivi dell'immagine altrui (commenti offensivi, minacce, osservazioni diffamatorie o discriminatorie, foto o video denigratori, videogiochi che contengano un'istigazione alla violenza, ecc.);

- contenuti riconducibili alla sfera sessuale: messaggi, immagini o video a sfondo sessuale, come foto di nudo o semi-nudo, ecc.

5.2.2. Come segnalare: quali strumenti e a chi.

Il personale della scuola, anche con l'ausilio del personale di assistenza tecnica, dovrà provvedere a conservare le eventuali tracce di una navigazione non consentita su internet o del passaggio di

materiali inidonei sui pc della scuola; la data e l'ora consentiranno di condurre più approfondite indagini; nel caso di messaggi, si cercherà di risalire al mittente attraverso i dati del suo profilo. Sia nel caso di chat che di messaggi di posta elettronica, l'insegnante dovrà copiare e stampare i messaggi per fornire le eventuali prove dell'indagine sugli abusi commessi. Tali prove saranno utili anche ad informare la famiglia dell'alunno vittima di abuso, il Dirigente scolastico e, ove si configurino reati, la Polizia Postale.
In ogni caso, sarà opportuna una tempestiva informazione delle famiglie in merito all'accaduto, anche per consentire ulteriori indagini e, in assenza di prove oggettive, di raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico ed, eventualmente, alla Polizia Postale. Qualora siano coinvolti più alunni, in qualità di vittime o di responsabili della condotta scorretta, tutte le famiglie degli alunni in questione saranno informate tempestivamente.

In base all'entità dei fatti la scuola comminerà le seguenti sanzioni:
1 .comunicazione scritta sul diario;
2. nota disciplinare sul Registro di classe;
3. convocazione formale dei genitori degli alunni, tramite segreteria, per colloquio con il coordinatore di classe;
4. convocazione delle famiglie tramite segreteria, per colloquio con il dirigente scolastico.

Per i reati più gravi la scuola si rivolgerà direttamente agli organi di polizia competenti.

5.3. Gestione dei casi

5.3.1. Definizione delle azioni da intraprendere a seconda della specifica del caso.

a) Casi di cyberbullismo:
Si definiscono bullismo tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o a volte un piccolo gruppo). Si tratta, pertanto, di una serie di comportamenti portati avanti ripetutamente nel tempo. Si parla di cyberbullismo quando queste forme di prevaricazione reiterate nel tempo si estendono anche alla vita online.
Tale specifica forma di bullismo ha caratteristiche peculiari:

- è pervasivo: il bullo può raggiungere la sua vittima in qualsiasi momento e in qualunque luogo;
- è un fenomeno persistente: il materiale messo online vi può rimanere per molto tempo;
- spettatori e cyberbulli sono potenzialmente infiniti: le persone che possono assistere agli atti di cyberbullismo sono potenzialmente illimitate.

Occorre tenere presente che il cyberbullo non è mai del tutto consapevole della gravità dei suoi comportamenti se non viene aiutato ad esserne consapevole.
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.

b) Casi di sexting:
Qualora ci si trovi di fronte a un caso di sexting si dovrà:

- informare i genitori degli alunni coinvolti;
- coinvolgere il referente di istituto dell'e-safety e gli operatori scolastici su quanto sta

accadendo;

- documentarsi opportunamente sulle norme giuridiche che regolano i comportamenti e le condotte sessuali in Italia;
- confrontarsi con esperti, ricorrendo allo sportello d'ascolto dell'istituto per capire come approfondire e affrontare il fenomeno con la classe;
- intraprendere con la classe attività mirate a riflettere sulla fiducia che ciascuno ripone negli altri e sul fenomeno del sexting, approfondendo casi e testimonianze.
- coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti riconducibili al sexting.

c) Casi di adescamento online o grooming:

Le tecnologie digitali consentono ai giovani di ampliare la propria rete di amicizie in modo quasi smisurato: non di rado gli adolescenti "concedono" la loro amicizia non solo a persone che conoscono direttamente, ma anche ad "amici di amici". Questo li espone a rischi notevoli, come quello di dare accesso a sconosciuti al loro mondo online e quindi a informazioni personali.
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., si dovrà:

- informare i genitori degli alunni coinvolti;
- coinvolgere il referente di istituto dell'e-safety e gli operatori scolastici su quanto sta accadendo;
- confrontarsi con esperti, anche ricorrendo allo sportello d'ascolto d'istituto, per capire come approfondire e affrontare il fenomeno con la classe;
- avviare dei percorsi di riflessione in classe sul concetto di fiducia;
- approfondire la situazione l'intera comunità scolastica.

Annessi

1. Procedure operative per la gestione delle infrazioni alla Policy

Le procedure, da applicarsi secondo i criteri dettati dalla policy, sono incluse nel Regolamento alunni e nel PTOF.

2. Procedure operative per la protezione dei dati personali

Le procedure sono incluse nel Regolamento disciplinare d'Istituto, sono parte integrante del PTOF; è obbligatoria la richiesta ai genitori per l'uso di immagini e video in attività didattica.

3. Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni

Le procedure, da applicarsi secondo i criteri e le modalità specifiche dettati dalla policy, sono incluse nel Regolamento disciplinare d'Istituto.

4. Protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi

Non vi sono specifici protocolli siglati, bensì ricorrenti forme di collaborazione nella prevenzione e contrasto del bullismo e del cyberbullimo.

Le referente — Il Dirigente scolastico

Proff.sse Ivana Massaro & Francesca Lanuara — dott.ssa Flora Scotto di Galletta