Ministero dell'istruzione, dell'università e della ricerca
Istituto Comprensivo Statale "*Tarra*"
Via Correggio, 80 - 20020 Busto Garolfo (MI)
Tel. 0331 569087 - Fax 0331 564462
Cod. Mec.: MIIC8DL00N - Cod. Fisc.: 84004070151
e-mail:miic8dl00n@istruzione.it -
e-mail:miic8dl00n@pec.istruzione.it
sito: http://www.ictarra.gov.it

POLICY di E-SAFETY

INDICE

Introduzione e processo di revisione pag. 1

- ✓ Scopo della Policy pag. 1

Stato di fatto: spazi fisici e virtuali disponibili nella Scuola pag. 2

- ✓ Strategie della scuola per garantire la sicurezza delle TIC pag. 3

Linee guida di buona condotta degli utenti pag. 4

- ✓ Altre tipologie di TIC pag. 7
- ✓ La Netiquette pag. 7
- ✓ Comunicazione con la Scuola pag. 8
- ✓ Garanzia e tutela della privacy pag. 9
- ✓ Sportello d'ascolto pag. 9

Didattica e azione dei docenti pag. 10

Prevenzione, rilevazione e gestione dei casi pag. 12

- ✓ Prevenzione pag. 12
- ✓ Rilevazione e gestione dei casi pag. 13

Diffusione della Policy di e-Safety pag. 16

INTRODUZIONE E PROCESSO DI REVISIONE

L'Istituto Comprensivo Statale "Tarra" ha ritenuto opportuno dotarsi di una *Policy di e-safety* per essere pronto a cogliere i cambiamenti sociali, economici, culturali e tecnologici del contesto in cui opera, in particolare per quanto riguarda la formazione dei cittadini del futuro, destinatati a vivere in un ambiente in cui tutto viene gestito attraverso l'utilizzo delle nuove tecnologie. Tali tecnologie diventano abilitanti, quotidiane, ordinarie, al servizio dell'attività scolastica e di tutti i suoi ambienti, coinvolgendo sia le attività orientate alla formazione e all'apprendimento, sia l'amministrazione, con ricadute estese al territorio.

Con questa *Policy* si vuole regolamentare l'uso di Internet, al fine di renderlo responsabile da parte di tutti gli utenti della Scuola e in modo tale da garantire la privacy all'interno dei plessi e degli uffici di segreteria. Inoltre, il curricolo pone l'accento sulle competenze digitali degli studenti, ai quali è richiesto di sapersi orientare nelle molteplici possibilità offerte da Internet, analizzando criticamente i materiali disponibili e scambiando informazioni ed esperienze in modo consapevole. Occorre in tal senso informare e formare, in particolare gli alunni, in merito a eventuali rischi e fornire misure atte a prevenirli, permettendo di beneficiare in sicurezza delle opportunità offerte da Internet e dalle TIC.

La *Policy* verrà revisionata e aggiornata annualmente, anche in base a eventuali variazioni delle dotazioni tecnologiche e dei protocolli dell'Istituto.

Scopo della Policy

Scopo del presente documento è quello di informare l'utenza al fine di garantire un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente. È pertanto fondamentale conoscere le norme comportamentali e le procedure per l'utilizzo delle TIC in ambiente scolastico, le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse a un uso non consapevole delle tecnologie digitali.

Tutti gli utenti devono essere consapevoli dei rischi cui sono esposti ogni volta che navigano in Internet: esiste, infatti, la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto la Scuola promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti. In questo contesto, gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a Scuola e di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, al fine di prevenire il verificarsi di situazioni potenzialmente pericolose. È comunque impossibile garantire una navigazione totalmente priva di rischi; negli ambienti scolastici, i docenti non possono assumersi le responsabilità che derivano da accessi accidentali e/o impropri a siti illeciti o dal reperimento e uso di materiali inappropriati.

STATO DI FATTO: spazi fisici e virtuali disponibili nella Scuola

Nell'Istituto "Tarra" la qualità e la quantità degli strumenti è in continua implementazione:

- la dotazione di nuovi strumenti informatici è un obiettivo prioritario, a partire dalla presenza della LIM in tutte le classi della Scuola Primaria e della Scuola Secondaria e di una LIM in ciascun plesso dell'Infanzia; ciò avverrà anche grazie al PON "Per la Scuola" 2014-2020 "Ambienti per la didattica digitale integrata", collegato all'Azione 4 del Piano Nazionale per la Scuola Digitale (PNSD), riguardante la realizzazione di Aule "Aumentate" dalla tecnologia;

- la realizzazione del cablaggio nei plessi del Comprensivo avverrà tramite la partecipazione al PON "Per la Scuola" 2014-2020 collegato all'azione 2 del PNSD "Cablaggio interno di tutte le scuole (LAN/WLAN)";

- il registro elettronico è in uso sia alla Scuola Secondaria che alla Scuola Primaria e verrà introdotto alla Scuola dell'Infanzia; al fine di garantirne una puntuale compilazione, le aule sono dotate di tablet e/o PC connessi alla rete Internet;

- i laboratori, in particolare quelli di informatica, sono presenti in vari plessi, dotati, in base alle attività che vi si svolgono, di connessione Internet attraverso rete WIFI e/o cavo, postazioni PC per alunni, LIM, videoproiettore;

- la segreteria, seguendo la normativa vigente, dal 1 gennaio 2016 ha raggiunto l'obiettivo della completa dematerializzazione; si presta particolare attenzione al potenziamento delle attrezzature informatiche, al mantenimento e costante aggiornamento della rete informatica e al potenziamento dei servizi digitali Scuola-famiglia-studente.

I referenti dei diversi laboratori hanno il compito di verificarne il funzionamento e il rispetto del regolamento. Gli insegnanti e il personale ATA sono tenuti a utilizzare con il massimo rispetto gli strumenti presenti nella Scuola, seguendo i regolamenti vigenti e minimizzando gli sprechi delle risorse a disposizione. I docenti sono responsabili dell'uso delle TIC nelle attività didattiche e hanno il fondamentale compito di responsabilizzare gli studenti, anche al fine di renderli consapevoli dell'importanza della salvaguardia di un bene comune, grazie alle corrette norme di utilizzo.

Strategie della scuola per garantire la sicurezza delle TIC

La Scuola prevede le seguenti strategie per garantire la sicurezza in rete:

- analizzare il fabbisogno formativo dei docenti e promuovere corsi di formazione inerenti all'uso sicuro e responsabile delle TIC e del web, sia nel loro uso privato, sia a Scuola;
- attuare, con la collaborazione di esperti esterni, incontri per presentare le modalità corrette di fruizione del web, il problema della tutela dei minori su Internet e sui social network, le problematiche e i rischi legati a bullismo, cyberbullismo e uso non responsabile del web a genitori, familiari ed eventuali persone interessate del territorio;
- far conoscere le problematiche psico-pedagociche correlate all'uso della rete;
- monitorare una tantum e/o al bisogno il sistema informatico (in particolare per ciò che concerne l'uso di Internet, cronologia, cookie…) da parte dei responsabili dei laboratori; le società informatiche che si occupano della manutenzione e assistenza dei dispositivi sono chiamate al bisogno e, a seconda dei casi, intervengo in loco o da remoto;
- garantire la costante presenza di un docente durante l'utilizzo di Internet o di altre TIC;
- installare firewall sull'accesso a Internet; aggiornare periodicamente il software antivirus; scansionare i dispositivi in cui si può sospettare la presenza di virus o malware;
- utilizzare penne USB, CD, DVD o altri dispositivi esterni personali solo se preventivamente autorizzati;
- monitorare eventuali problemi riscontati durante l'uso delle TIC o della rete e prevedere piani d'azione per risolvere i più frequenti;
- adottare tutti gli accorgimenti possibili per evitare comportamenti contrari al presente regolamento e alla normativa vigente:
    - scaricare file protetti da copyright e violare le leggi sui diritti d'autore;
    - visitare siti non inerenti all'attività didattica, usare la rete per interessi privati e personali;
    - alterare i parametri di protezione dei dispositivi utilizzati.

LINEE GUIDA DI BUONA CONDOTTA DEGLI UTENTI

Ferme restando le strategie sistematiche messe in atto dalla Scuola di cui al precedente paragrafo, ciascun utente connesso alla rete deve:

- rispettare il presente regolamento e la legislazione vigente;
- tutelare la propria privacy, quella degli altri utenti adulti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui ha accesso;
- rispettare la cosiddetta *netiquette* (regole condivise che disciplinano il rapportarsi tra utenti della rete, in contatto attraverso siti, forum, mail, blog, newsgroup…).

Di seguito si dettagliano i comportamenti da tenere distinguendo attività e utenti.

Durante l'attività didattica, ogni **docente** può avvalersi degli strumenti a disposizione nell'aula docenti, nelle aule o nei laboratori e deve:

- leggere, comprendere e aderire a questa *Policy*;
- aver cura degli strumenti in dotazione, in particolare spegnendo correttamente tablet, PC, LIM e proiettori al termine del periodo di utilizzo o, in ogni caso, delle lezioni;
- accedere al registro elettronico attraverso il tablet, che il docente della prima ora preleva dall'armadietto apposito, o dal pc presente in classe e provvedere a registrare assenze, giustificazioni, ritardi, nonché aggiornare durante le ore successive le entrate posticipate e uscite anticipate. Il tablet e il pc devono essere custoditi, tenuti fuori dalla portata dei ragazzi e, nel caso dei tablet, riposti nell'armadietto dal docente dell'ultima ora. Nei vari spostamenti della classe in altri luoghi della Scuola, sarà cura del docente portare con sé il tablet;
- compilare nell'arco delle 24 ore rispetto alla lezione e aggiornare costantemente il registro elettronico, comprese le valutazioni; sarà inoltre cura del docente custodire la segretezza della password;
- evitare di divulgare agli alunni le credenziali di accesso alla rete WIFI;
- evitare di installare e utilizzare software personali o senza autorizzazione, o modificare le impostazioni dei dispositivi, in particolare PC, della Scuola;
- assumersi la responsabilità della tracciabilità dell'utilizzo e del mantenimento in buono stato della strumentazione tecnologica utilizzata, segnalando celermente eventuali malfunzionamenti ai responsabili secondo le modalità previste;

- evitare di salvare sulla memoria delle postazioni utilizzate file contenenti dati personali e/o sensibili;
- evitare di lasciare memorizzate credenziali, email, file personali sui dispositivi o sui server; assicurarsi di non lasciare la postazione prima di aver effettuato il logout;
- salvare file non sul desktop, ma in cartelle personali o di classe; i file di lavoro non salvati in tal modo saranno eliminati da parte di chi si occupa del corretto funzionamento dei dispositivi;
- per utilizzare i laboratori, compilare il registro di prenotazione, presente in bidelleria, dove sono disponibili anche le chiavi; indicare classe, giorno, ora, cognome, eventuali malfunzionamenti riscontrati prima, durante o alla conclusione dell'attività svolta. Le chiavi verranno consegnate al docente che dovrà firmare all'atto della consegna e nel momento in cui le restituisce. L'accesso all'aula non è consentito agli alunni se non accompagnati da docenti. Prima di lasciare l'aula, accertarsi che tutti i PC siano stati spenti nel modo corretto. Eventualmente, si dovrà compilare il "Modulo per la segnalazione di problemi riguardanti i computer del laboratorio di informatica";
- controllare l'uso corretto dell'aula e dei computer (mouse, tastiera, monitor), e assicurarsi che non vengano introdotti cibi o bevande;
- illustrare agli alunni le regole di utilizzo del presente documento e informarli in merito alle sanzioni disciplinari previste per chi incorresse in violazioni consapevoli delle norme adottate;
- informare gli alunni sui rischi cui sono potenzialmente esposti e sul corretto uso della rete (motori di ricerca, piattaforme in uso – Moodle, Onfire…–, registro elettronico);
- premurarsi che l'accesso degli alunni alla rete avvenga sempre sotto la sua supervisione;
- vigilare, durante la navigazione, che tutti usino in modo corretto la rete, guidandoli e fornendo costanti indicazioni su ciò che è richiesto dalla *netiquette*;
- guidare gli alunni nelle ricerche online: fornire obiettivi chiari, proporre indirizzi web, parole chiave per la ricerca, prediligendo siti istituzionali, creati *ad hoc* per la didattica; il docente deve, inoltre, aver preventivamente visionato i siti che andrà a proporre, verificandone accuratamente la sicurezza e il rispetto dei diritti di proprietà intellettuale;
- segnalare ai responsabili l'uso di siti internet non compatibili con la politica educativa della Scuola.

Durante l'attività didattica, gli **alunni** devono:

- leggere, comprendere e aderire a questa *Policy*;

- accedere al laboratorio di informatica solo se accompagnati da docenti e seguire le indicazioni fornite in merito all'utilizzo delle TIC (LIM, laboratori didattici, PC, tablet…). Saranno previste eccezioni per l'uso dei dispositivi da parte degli alunni con BES, per i quali è possibile l'utilizzo del PC personale e la registrazione delle lezioni, regolamentati dai rispettivi PEI e PDP e dalla normativa vigente;
- accedere agli ambienti di lavoro con le proprie credenziali, senza divulgarle, e archiviare i propri file in modo ordinato, così da essere facilmente rintracciabili, all'interno di una cartella personale nel Server della didattica o su supporto esterno;
- accedere alla rete solo in presenza e previa autorizzazione del docente responsabile dell'attività;
- evitare di utilizzare la strumentazione della Scuola a scopi personali, ludici e/o ricreativi;
- evitare di eseguire tentativi di modifica della configurazione di sistema dei dispositivi;
- evitare di utilizzare dispositivi esterni personali senza aver preventivamente acquisito l'autorizzazione da parte del docente;
- chiudere correttamente la propria sessione di lavoro.

I **genitori** sono tenuti a

- leggere, comprendere e promuovere la *Policy* con i loro figli;
- controllare frequentemente il registro elettronico;
- interessarsi al modo in cui i figli usano la tecnologia e guidarli verso un comportamento responsabile e sicuro;
- consultare e collaborare con la Scuola se dovessero sorgere preoccupazioni riguardo l'uso della tecnologia da parte del figlio.

Altre tipologie di TIC

Lo studente può utilizzare i *device* di sua proprietà al di fuori dei locali scolastici o comunque di pertinenza della Scuola (cortile). Durante l'orario scolastico, agli studenti non è permesso l'uso della telefonia mobile e di altri strumenti informatici di loro proprietà; l'eventuale utilizzo durante una specifica attività didattica, inserita nel PTOF, deve essere autorizzata e costantemente supervisionata dal docente di classe. Come già precedentemente evidenziato, si possono prevedere eccezioni nel caso di alunni con BES.

Le infrazioni e le sanzioni relative a un uso improprio delle TIC da parte degli studenti sono declinate nel *Regolamento d'Istituto*.

La Netiquette

Chiunque si trovi a utilizzare le TIC, Internet e i servizi offerti dalla rete, deve attenersi a una serie di regole che disciplinano il comportamento degli utenti nel rapportarsi con gli altri; tali norme costituiscono la cosiddetta *Netiquette*, una sorta di Galateo della Rete.

Si riportano alcune delle norme su cui si intende sensibilizzare in modo particolare l'utenza:

- in rete la comunicazione avviene principalmente attraverso testi, con conseguente rischio di essere fraintesi: talvolta, nei contesti opportuni, le *emoticon* possono aiutare a chiarire il tono del messaggio; risulta opportuno quotare i messaggi originari per facilitare la comprensione delle risposte;
- evitare di inviare messaggi ripetitivi, inutili o inopportuni (spam); evitare altresì l'invio di messaggi pubblicitari, catene o comunicazioni non espressamente richieste;
- in rete si possono esprimere la propria opinione e le proprie idee, sempre rispettando tutti gli interlocutori e i fruitori del messaggio; la rete offre la possibilità di entrare in contatto con milioni di utenti, dei quali vanno rispettati la nazionalità, la cultura, la religione, il sesso: non sono ammesse forme di razzismo o discriminatorie;
- è necessario rispettare gli interlocutori virtuali: i loro tempi nella risposta, che non andrà mai pretesa, il loro interesse o meno a quanto proposto; gli errori di digitazione, di grammatica o di sintassi non devono essere stigmatizzati, l'importante è che la trasmissione del messaggio avvenga con successo. Si ricorda che lo scrivere in maiuscolo equivale a urlare: non abusarne;
- scegliere forum, social, community, chat, mailing list, etc, cui si intende partecipare in base agli argomenti che interessano o alle esigenze emerse; partecipare rispettandone le regole e gli interventi dei moderatori;
- l'espressione del proprio parere deve avvenire in modo pacato, così da non provocare dure reazioni nelle persone con cui si comunica ed evitare "guerre di opinione";

- evitare di sfruttare le proprie competenze digitali per violare siti o profili di altri utenti, pubblicare contenuti o conversazioni private, condividere fotografie, video o altri file di utenti terzi senza averne il consenso;
- curare la propria reputazione digitale, valutando sempre con la massima attenzione ciò che si vuole comunicare, pubblicare e condividere;
- rispettare la privacy degli altri utenti: ognuno può scegliere cosa pubblicare e condividere delle informazioni che lo riguardano;
- evitare di rivelare dettagli, informazioni personali o dati sensibili propri o altrui;
- evitare di credere a tutto ciò che viene detto sulla rete e diffidare di chi chiede informazioni personali o incontri dopo poco tempo che si è entrati in contatto: non sempre è possibile avere la certezza dell'identità della persona con la quale si sta comunicando.

Comunicazione con la Scuola

La Scuola promuove una comunicazione chiara e trasparente con il personale, le famiglie e il territorio, in particolare attraverso:

- il **sito istituzionale,** www.icstarra.gov.it, costantemente aggiornato, che fornisce un'informazione puntuale e trasparente su tutte le attività e la documentazione relative alla Scuola;
- il **registro elettronico**, costantemente aggiornato dai docenti, sul quale le famiglie possono controllare assenze, voti, annotazioni e schede di valutazione;
- la **posta elettronica**, canale preferenziale per la trasmissione di informazioni e comunicazioni tra tutti gli utenti.

La Scuola fornisce un supporto alle famiglie per le iscrizioni online ai diversi ordini di Scuola, fatta eccezione per quanto riguarda la Scuola dell'Infanzia, mediante postazioni informatiche dedicate e personale applicato di segreteria.

La Scuola, conseguentemente alla dematerializzazione, si è dotata di un sistema per la firma grafometrica, predisposto per tutti gli utenti.

Garanzia e tutela della privacy

L'Istituto opera a ogni livello rispettando tutte le normative vigenti in merito alla tutela della privacy, come indicato sul sito istituzionale http://www.icstarra.gov.it/wordpress/privacy/.

La compilazione di un modello riguardante il trattamento immagini e audiovisivi degli alunni è richiesta:

- a chi si iscrive all'ordine successivo oppure per la prima volta nell'Istituto durante la compilazione del modulo di iscrizione;
- a ciascun alunno all'inizio di ogni anno scolastico, tramite il diario o attraverso l'apposita modulistica presente sul sito istituzionale.

Sportello d'ascolto

Tra le misure di prevenzione che la Scuola mette in atto per la prevenzione del disagio, anche per quanto riguarda l'uso delle TIC, di Internet e le relazioni virtuali che nella rete si possono sviluppare, si registra la presenza di uno "Sportello di ascolto", rivolto a tutti gli allievi, articolato in colloqui individuali e/o collettivi, con l'obiettivo di migliorare il benessere personale e scolastico di ogni singolo alunno, mediante un'attività di supporto della sfera emotiva, relazionale e comportamentale. È previsto, al suo interno, uno spazio riservato ai docenti e genitori al fine di individuare strategie efficaci per affrontare problematiche tipiche dell'età adolescenziale.

DIDATTICA E AZIONE DEI DOCENTI

L'Istituto, come evidenziato nel Piano Triennale dell'Offerta Formativa, pone particolare attenzione allo sviluppo della competenza digitale dei propri studenti, in linea con quanto previsto dal Piano Nazionale per la Scuola Digitale (PNSD). Questa competenza non può essere sciolta dalle competenze sociali e civiche che ogni alunno deve maturare, soprattutto per gli aspetti relazionali da esse implicati: l'ascolto, il rispetto reciproco, la capacità di vivere insieme; in tal modo ci si prefigge di prevenire eventuali fenomeni di disagio giovanile (bullismo, cyberbullismo, violenza, discriminazioni, uso di sostanze stupefacenti…).

La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni, nonché per comunicare e partecipare a reti collaborative tramite Internet. Si pone quindi enfasi sulla capacità di esplorare e affrontare in modo flessibile situazioni tecnologicamente nuove, adeguando le performance ai diversi contesti in cui si opera, in modo tale da:

- saper analizzare e valutare criticamente i dati e le informazioni con cui ci si confronta durante la navigazione online e l'uso delle TIC;
- saper sfruttare le potenzialità offerte dalle TIC per la risoluzione di problemi;
- saper costruire e condividere le conoscenze acquisite, sviluppando una consapevole responsabilità in merito ai dati personali e alla tutela della privacy, con particolare attenzione ai diritti e doveri reciproci degli utenti.

La competenza digitale è data dalla fusione delle dimensioni:

- etica, inerente alla responsabilità sociale, al sapere relazionarsi con gli altri utenti, al tenere dei comportamenti adeguati alle circostanze in cui ci si può imbattere e alla tutela della propria persona, per preservare la quale è necessario sapersi schermare dai possibili rischi;
- tecnologica, il saper individuare gli usi e i punti di forza dei dispositivi in uso e, quindi, scegliere i *device* e i mezzi adeguati per risolvere problemi;
- cognitiva, grazie alla quale è possibile saper leggere, selezionare e valutare dati, attraverso modelli astratti che conducano a un'analisi critica degli stessi al fine di individuare, tra tutte quelle offerte dalla rete, le informazioni attendibili e pertinenti al compito affidato.

Per perseguire questi traguardi, i docenti adottano, come supporto alle attività scolastiche, le tecnologie educative e didattiche a disposizione, quali LIM, libri di testo, risorse multimediali; fondamentale è infatti la didattica mediale, grazie alla quale i media sono visti come un supporto fondamentale per un apprendimento disciplinare multimediale. Ai docenti spetta anche il compito di educare ai media, intorno ai quali sviluppare una riflessione critica e una sperimentazione creativa, approfondendo le dinamiche che regolano il sistema dei media stessi, la decodifica dei messaggi e la conoscenza dei linguaggi mediali. Ciò è realizzabile grazie a un approccio costruttivista, basato sull'apprendimento, e a metodi di insegnamento quali *flipped classroom*, EAS…

L'Istituto, coerentemente con quanto previsto dal PNSD, attiva dei percorsi di formazione rivolti ai docenti per acquisire le competenze necessarie.

PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

Prevenzione

L'Istituto si prefigge come obiettivo quello di fornire a tutta l'utenza le competenze necessarie al fine di poter tenere comportamenti responsabili e corretti nella fruizione delle TIC e della rete, così da poter prevenire i rischi in cui ci si può imbattere.

Per quanto riguarda l'uso delle TIC, tutto il personale in servizio presso la Scuola, gli alunni e le loro famiglie sono informati e formati in merito alle modalità per utilizzare in modo sicuro, negli ambienti scolastici o all'esterno, i diversi *device*, quali tablet, pc, smartphone; sono fornite indicazioni su come gestire impostazioni di cronologia, cookie, cache, firewall, malware e virus in genere.

Fondamentale è anche diffondere le nozioni volte a raggiungere una navigazione sicura, corretta e responsabile online, per quanto concerne:

- l'uso di siti e piattaforme istituzionali, compresi il sito della Scuola, il registro online e le piattaforme usate durante le attività didattiche;
- la gestione degli account, con attenzione alla conservazione delle credenziali di accesso;
- le misure di sicurezza per la fornitura dei dati personali, ponendo attenzione alle situazioni in cui ciò è sconsigliato o poco opportuno;
- la gestione e la netiquette delle caselle di posta elettronica in genere e delle mailing list, anche per ciò che riguarda la possibilità di imbattersi in comunicazioni fraudolente;
- le regole per l'upload e il download in sicurezza di qualsiasi tipo di file;
- la gestione delle relazioni sui social network, nelle chat e nelle applicazioni di instant messaging, soprattutto a proposito della condivisione e pubblicazione di foto, video, informazioni personali, conversazioni, etc;
- i rischi di entrare in siti non opportuni, pornografici, di reclutamento a fini illegali, fraudolenti;
- i rischi più diffusi in rete, anche a causa di un utilizzo non responsabile della stessa, in particolare:
    - cyberbullismo;
    - sexting;
    - grooming.

- la normativa vigente sulla privacy e sulle procedure di dematerializzazione messe in atto dalla Scuola.

Rilevazione e gestione dei casi

L'intera utenza della Scuola, in particolare personale docente e genitori, deve essere costantemente formata, informata e aggiornata sui fenomeni del bullismo e del cyberbullismo. A tal fine, si è in contatto con una rete di supporto territoriale, formata da diversi enti, quali la Cooperativa Stripes, Hakuna Matata, il Comune, attraverso l'ufficio Servizi Sociali, e altri centri di associazione o associazioni del territorio, nonché con la helpline di Generazioni Connesse, gestita dal Telefono Azzurro.

I docenti sono opportunamente formati e aggiornati sulle modalità e gli indicatori per riconoscere eventuali casi o situazioni a rischio e sulle procedure da seguire.

Chiunque entri in possesso di dati certi deve avere la possibilità di denunciarli in forma tutelata: il denunciante non deve correre rischi e deve avere tutte le possibili tutele.

Nel momento in cui si è a conoscenza di situazioni di bullismo o cyberbullismo:

- il docente deve avvisare immediatamente il fiduciario del plesso e la dirigenza scolastica;
- il docente deve stendere un verbale dell'episodio, nel quale vengono riportate le situazioni problematiche rilevate;
- si convoca la famiglia per informarla dell'accaduto;
- il docente svolge un colloquio approfondito, in separata sede, sia con la vittima che con il bullo o cyberbullo, al fine di acquisire informazioni aggiuntive; il docente è tenuto a verbalizzare le informazioni apprese;
- il docente deve stendere un verbale del colloquio, nel quale vengono riportate le informazioni rilevate;
- a seconda dei casi, si informeranno i servizi sociali e/o la Polizia Postale;
- in caso di eventi particolarmente gravi o con profili che si possono presumere penali, è obbligatorio ricorrere all'autorità giudiziaria;
- gli studenti protagonisti di atti di bullismo o cyberbullismo sono tenuti a comprendere la gravità degli atti compiuti; devono essere sanzionati come da regolamento e, contestualmente, devono essere obbligati a comportamenti attivi di natura risarcitoria e riparatoria, volti al perseguimento di una finalità educativa (cfr. Circolare 15/05/2007, MPI);
- a livello formativo, i docenti tengono conto dell'accaduto nel corso del processo didattico.

Si ricorda che, in caso di necessità ci si può rivolgere ai seguenti servizi, gestiti da Telefono Azzurro (http://www.azzurro.it/it/sostegno), come suggerito dalla *Helpline* di Generazioni Connesse (http://www.generazioniconnesse.it/index.php?s=38):

- *Linea di ascolto* 1.96.96, attiva 24 ore su 24, 365 giorni all'anno;
- *Chat,* attiva dalle 8.00 alle 22.00 in settimana, dalle 8.00 alle 20.00 il sabato e la domenica.

Tali canali accolgono qualsiasi richiesta d'ascolto e di aiuto da parte di bambini e ragazzi fino ai 18 anni, o da parte di adulti che si vogliono confrontare su situazioni di disagio/pericolo che vedono coinvolti dei minori:

- uso sicuro di Internet e dei social network;
- adescamento online/grooming;
- pedopornografia;
- cyberbullismo;
- sexting, pornografia e sessualità online degli adolescenti;
- gioco d'azzardo online;
- violazione della Privacy;
- furto di identità in rete;
- esposizione a contenuti nocivi online;
- dipendenza da Internet;
- esposizione a siti violenti, razzisti, che invitano al suicidio o a comportamenti alimentari scorretti (pro-anoressia e pro-bulimia);
- dipendenza da shopping online;
- videogiochi online non adatti ai ragazzi.

Il servizio di *Helpline* è riservato, gratuito e sicuro, dedicato ai ragazzi e alle famiglie, che possono trovarvi un consulto con professionisti qualificati relativamente a dubbi, domande o problemi legati all'uso delle nuove tecnologie digitali e alla sicurezza in rete.

È possibile, inoltre, usufruire del servizio *Hotline*, reperibile all'indirizzo http://www.generazioniconnesse.it/index.php?s=37, che raccoglie e dà corso a segnalazioni, inoltrate anche in forma anonima, riguardanti contenuti pedopornografici, illegali o dannosi presenti online. I servizi messi a disposizione dal Safer Internet Center sono:

- *Clicca e segnala*, di Telefono Azzurro;
- *Stop-it*, di Save the Children.

Dopo che sarà stata ricevuta una segnalazione, gli operatori provvederanno a coinvolgere, al bisogno, le autorità competenti.

Per segnalare contenuti inopportuni visionati sui media si può far riferimento al sito del CoReCom (Comitato Regionale per le Comunicazioni) all'indirizzo http://www.corecomlombardia.it/opencms/index.html.

Anche la Polizia Postale e delle Comunicazioni https://www.commissariatodips.it/ è attualmente impegnata in attività a sostegno delle navigazione protetta dei minori ed è competente a ricevere segnalazioni in merito a qualsiasi tipo di reato informatico.

DIFFUSIONE DELLA POLICY DI E-SAFETY

La *Policy* e le regole in essa contenute verranno approvate dal Dirigente Scolastico, dal Collegio dei Docenti, dal Consiglio di Istituto e pubblicate online sul sito istituzionale della Scuola.

Il personale scolastico è tenuto alla lettura e sottoscrizione della *Policy*, nonché allo sviluppo delle linee guida e all'applicazione scrupolosa delle istruzioni sull'uso sicuro e responsabile della rete.

Gli studenti sono informati dei contenuti della Policy attraverso il *Patto di Corresponsabilità* e costantemente supportati per un uso responsabile e consapevole delle TIC e della rete. Gli studenti e i loro genitori/tutori devono firmare il documento.

I genitori o i tutori sono invitati a prestare la massima attenzione ai principi e alle regole contenuti in questo documento; si richiede un impegno costante affinché siano rispettate anche in ambito extrascolastico, assistendo i minori nel momento dell'utilizzo della rete e adottando tutti i sistemi di sicurezza per diminuire i possibili rischi della rete.