



Ministero dell'Istruzione, dell'Università e della Ricerca
Ufficio Scolastico Regionale per il Lazio
Istituto Comprensivo "VIA DE FINETTI"
Via B. De Finetti 170/b - 00134 ROMA - Tel.06/50162010

E-Safety Policy

Documento redatto da:

Silvia Liuzzi

Ilaria Palma

Isabella Pannoncini

Vincenzo Piccolo

Claudia Serani

Anno Scolastico 2016-2017

INDICE

1. Introduzione

- 1.1.Scopo della Policy
- 1.2.Ruoli e Responsabilità
- 1.3.Condivisione e comunicazione della Policy all'intera comunità scolastica
- 1.4.Gestione delle infrazioni alla Policy
- 1.5.Monitoraggio dell'implementazione della Policy e suo aggiornamento
- 1.6.Integrazione della Policy con Regolamenti esistenti

2. Formazione e Curricolo

- 2.1. Curricolo sulle competenze digitali per gli studenti
- 2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica
- 2.3. Sensibilizzazione delle famiglie
- 2.4. Gli strumenti TIC a supporto dell'inclusione e della partecipazione

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

- 3.1. Accesso ad internet: filtri, antivirus e sulla navigazione
- 3.2. Gestione accessi (password, backup, ecc...)
- 3.3. E-mail
- 3.4. Blog e sito web della scuola
- 3.5. Social network
- 3.6. Protezione dei dati personali
- 3.7 Gestione e utilizzo dei laboratori informatici

4. Strumentazione personale

- 4.1. Per gli studenti
- 4.2. Per i docenti e il personale della scuola

5. Prevenzione, rilevazione e gestione dei casi

- 5.1. Prevenzione
 - Rischi
 - Azioni
- 5.2. Rilevazione
 - Che cosa segnalare
 - Come segnalare: quali strumenti e a chi.
 - Come gestire le segnalazioni.
- 5.3. Gestione dei casi
 - Definizione delle azioni da intraprendere a seconda della specifica del caso.

Annessi

1. Procedure operative di rilevazione e gestione dei casi
2. Scheda di segnalazione
3. Scheda per la rilevazione di violazione delle disposizioni sulla strumentazione personale
4. Schema riepilogativo delle situazioni gestite legate ai rischi online

1. Introduzione

L'Istituto Comprensivo "Via De Finetti" è situato nel quartiere Fonte Laurentina del comune di Roma, e comprende tre plessi di cui due di scuola primaria e uno di scuola secondaria di 1° grado. Altri due plessi apriranno nell'a.s. 2017-2018: la scuola dell'infanzia e un plesso di scuola secondaria di 1° grado.

La scuola è l'unica istituzione statale presente nel quartiere di Fonte Laurentina e Castel di Leva. L'utenza è eterogenea: generalmente appartenente a un ceto medio, sono presenti anche alunni provenienti da famiglie socialmente e culturalmente più svantaggiate.

L'I.C. "Via De Finetti" intende utilizzare in misura diffusa le nuove tecnologie, la didattica laboratoriale e l'apprendimento collaborativo. Ha partecipato ai Bandi del Miur nell'a.s. 2015-2016 per due progetti PON: -Infrastrutture, rete Lan, WLAN (finanziato per plesso via Capelli) -Ambienti digitali (finanziato per la scuola secondaria 1° grado).

Lo sviluppo e l'integrazione dell'uso delle TIC nella didattica, nonché la presenza sempre più diffusa delle tecnologie digitali nella vita di tutti i giorni, pone nuove attenzioni dal punto di vista del loro uso sicuro, consapevole e positivo.

Tra le priorità del PDM della scuola vi è quella di incrementare la diffusione dell'innovazione metodologica nell'insegnamento-apprendimento, inoltre tra gli obiettivi di processo individuati nel RAV vi è quello di diffondere una didattica laboratoriale anche attraverso un maggior utilizzo delle TIC.

Nel corrente anno scolastico l'Istituto Comprensivo "Via De Finetti", avendo aderito al progetto "Generazioni Connesse" del SIC (Safer Internet Center), promosso dal MIUR in collaborazione con la Comunità Europea, ha intrapreso una serie di iniziative per favorire negli alunni un uso corretto e sicuro delle nuove tecnologie e per insegnare loro un atteggiamento corretto e consapevole finalizzato ad ottenere il massimo dei vantaggi senza correre i rischi legati alla rete.

Nell'ambito di questo progetto il nostro Istituto ha redatto un documento (*e-safety Policy*) mediante il coinvolgimento di tutti gli interlocutori-protagonisti per ridefinire una procedura comune e delle norme comportamentali per l'utilizzo delle tecnologie digitali e della rete. E' stato fondamentale definire delle misure chiare e precise per prevenire usi non coscienti delle tecnologie digitali e per favorire la crescita consapevole delle competenze digitali.

1.1.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, siano essi docenti o alunni, 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.

1.2. Ruoli e responsabilità (che cosa ci si aspetta da tutti gli attori della comunità scolastica)

a) Dirigente scolastico:

Il ruolo del Dirigente scolastico nel promuovere l'uso consentito delle tecnologie e di internet include i seguenti compiti:

- garantire la sicurezza (tra cui la sicurezza on line) dei membri della comunità scolastica;
- garantire che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, un utilizzo positivo e responsabile delle Tecnologie dell'informazione e della Comunicazione (TIC);
- garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on line.

b) Animatore digitale, il team dell'innovazione, funzione strumentale per l'innovazione e referenti dei laboratori informatici :

Il ruolo delle figure in oggetto include i seguenti compiti:

- stimolare la formazione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on line e alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola;
- assicurare che gli utenti possano accedere alla rete della scuola per scopi istituzionali e consentiti (istruzione e formazione);
- coinvolgere la comunità scolastica (alunni, genitori e altrui attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".

c) Direttore dei servizi generali e amministrativi

Il ruolo del Direttore dei servizi generali e amministrativi include i seguenti compiti:

- assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni.

d) Docenti:

Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere formativo all'Animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- segnalare al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.

e) Allievi:

Il ruolo degli alunni include i seguenti compiti:

- essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali;
- comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori;
- conoscere e comprendere le politiche sull'uso di dispositivi mobili e di macchine fotografiche digitali, capire le politiche di utilizzo delle immagini ed essere consapevoli del significato e della gravità del cyberbullismo.

- capire l'importanza di adottare buone pratiche di sicurezza informatica in tutti i momenti della vita, a tutela dell'incolumità propria e altrui e per evitare di perpetrare reati punibili sia a livello scolastico sia da parte della magistratura.

f) Genitori:

Il ruolo dei genitori degli alunni include i seguenti compiti:

- Sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle Tecnologie dell'informazione e delle Comunicazioni nella didattica;
- controllare l'utilizzo del PC e di internet dei propri figli.

g) Personale ATA

Il personale ATA è tenuto ad assicurarsi di:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- aver letto, compreso e sottoscritto la presente policy;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'animatore digitale per le opportune indagini / azioni / sanzioni.

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

Per evitare che l'adozione di questa policy rappresenti un mero atto formale, l'Istituto si impegna a prendere spunto da essa come base di partenza per una serie di azioni e iniziative. A partire dalla pubblicazione sul sito della scuola, si possono ipotizzare per esempio:

- Per il **corpo docente**, discussione collegiale sui contenuti, sulle pratiche indicate e su come inserire nel curriculum le tematiche di interesse della policy; un confronto collegiale, su base annuale, circa la necessità di apportare modifiche e miglioramenti alla policy vigente; elaborazione di protocolli condivisi di intervento.
- Per la **componente studentesca**, la discussione in classe della policy nei primi giorni di scuola, con particolare riguardo al protocollo di accoglienza per le nuove classi prime; l'inserimento di un estratto di questo documento nel diario scolastico e in particolare dei comportamenti da attuare in caso di bisogno.
- Per i **genitori**, l'organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare.

1.4. Gestione delle infrazioni alla policy

a) Disciplina degli alunni

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

- un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;

- l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;
- la condivisione di immagini intime o troppo spinte;
- la comunicazione incauta e senza permesso con sconosciuti;
- il collegamento a siti web non indicati dai docenti;

In un Istituto Comprensivo devono essere previsti, da parte dei docenti, provvedimenti, disciplinari, proporzionati all'età e alla gravità del comportamento, quali:

- il richiamo verbale;
- il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);
- il richiamo scritto con annotazione sul diario;
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente scolastico.

b) Disciplina del personale scolastico

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

- un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti.

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

c) Disciplina dei genitori

Alcuni comportamenti e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte dei propri figli a scuola:

- una posizione del computer in una stanza o in un posto non visibile a tutti quando viene utilizzato dal proprio figlio;
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone;
- un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei;
- un utilizzo del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria indirizzi o contenuti non idonei.

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

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

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

1.5. Monitoraggio dell'implementazione della policy e suo aggiornamento

Le regole relative all'accesso ad Internet vengono approvate dal Collegio dei Docenti e dal Consiglio di Istituto e pubblicate sul sito della scuola. Gli alunni vengono informati del fatto che l'utilizzo di Internet è monitorato e vengono date loro istruzioni per un uso responsabile e sicuro. Il personale scolastico riceve una copia del Regolamento, che viene sottoscritta e osservata scrupolosamente. Tutto il personale scolastico, pertanto, è coinvolto nel monitoraggio dell'utilizzo di Internet, nello sviluppo delle linee guida e nell'applicazione delle istruzioni sull'uso sicuro e responsabile di Internet.

1.6. Integrazione della policy con regolamenti esistenti

Il "Regolamento per l'uso delle risorse tecnologiche e di rete" è stato allegato al Regolamento di Istituto e inserito nel sito web della scuola. I genitori vengono informati della pubblicazione del "Regolamento per l'uso delle risorse tecnologiche e di rete" della scuola e possono prenderne visione sul sito della scuola e partecipare ad attività di formazione.

2. Formazione e Curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

Le TIC e Internet sono un elemento essenziale nella vita di oggi. La scuola ha il dovere di fornire agli studenti l'accesso a questi strumenti come parte della loro esperienza di apprendimento e di far maturare in loro le competenze per una proficua cittadinanza digitale.

Le competenze digitali devono essere certificate sulla base del seguente profilo:

- Al termine della scuola primaria: *usa le tecnologie in contesti comunicativi concreti per ricercare dati e informazioni e per interagire con soggetti diversi.*
- Al termine della scuola secondaria di primo grado: *usa con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo.*

Tutto questo potrà avvenire mediante:

- a) Inserimento dell'uso delle TIC nel curricolo sia a livello disciplinare sia a livello interdisciplinare;
- b) Educazione ai media (riflessione critica e sperimentazione creativa) approfondendo le dinamiche che regolano il sistema dei media e lavorando sulla decodifica dei messaggi e la conoscenza dei linguaggi mediali;
- c) Educazione con i media mediante l'utilizzo di video educativi, utilizzo delle LIM, di tablet e smartphone a scuola;
- d) Dalla quarta elementare in poi almeno 2 incontri di formazione in plenaria strutturati per fasce d'età e tenuti da esperti del settore (Polizia postale, psicologi, etc...);
- e) Educazione all'affettività e alla relazione attraverso un incontro formativo con scambio di esperienze, tra alunni di scuola primaria e di scuola secondaria di primo grado su tematiche legate al rispetto e alla tolleranza;
- f) Condivisione e comunicazione della Policy di e-safety a tutti gli alunni in cui si specifica che la rete, l'uso di Internet e di ogni dispositivo digitale sarà controllato dagli insegnanti e utilizzato solo previa autorizzazione;
- g) Affissione dell'elenco delle regole per la sicurezza on-line in tutte le aule e laboratori con accesso a internet.

2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica e sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

Diversi membri del corpo docente partecipano costantemente a corsi di formazione anche nell'ambito del PNSD, ad iniziative organizzate dall'istituto o da altri enti e, sebbene l'evoluzione continua della tecnologia determini una rapida obsolescenza delle attrezzature in dotazione e delle conoscenze in materia, possiedono una buona base di competenze. D'altronde la formazione dei docenti sull'utilizzo delle TIC nella didattica è fondamentale per la buona riuscita della E- SafetyPolicy che pertanto deve prevedere:

- a) Organizzazione di due o più incontri nel corso dell'anno scolastico di autoaggiornamento e

condivisione di buone pratiche realizzate da docenti dell'Istituto;

- b) Diffusione tempestiva e capillare di corsi, convegni e seminari per la formazione personale cercando altresì di agevolare il personale che intenda parteciparvi;
- c) Organizzazione di uno o più eventi formativi all'interno dell'istituto mediante il supporto dell'Animatore digitale e del Team digitale e/o partecipazione alle iniziative promosse dalle scuole polo;
- d) Adesione a progetti appositi di formazione presentati da enti e associazioni;
- e) Condivisione e comunicazione della Policy di e-safety in cui si specifica la linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet;
- f) Creazione di una sezione sul sito dell'Istituto per la messa a disposizione e la condivisione della Policy di e-safety e di materiali informativi sulla sicurezza in internet, l'approfondimento personale, le attività con gli studenti, gli incontri con i genitori, ecc.

2.3. Sensibilizzazione delle famiglie

L'Istituto ha già attivato e continua ad attivare iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete promuovendo la conoscenza delle numerose situazioni di rischio online.

Per una maggiore consapevolezza in tal senso, è necessario prevedere:

- a) Incontri fra docenti e genitori per la diffusione del materiale informativo messo a disposizione dai siti specializzati, dalla piattaforma di "Generazioni Connesse" e dalle forze dell'ordine;
- b) Diffusione delle informazioni e delle procedure contenute nel documento della Policy e-safety per prevenire i rischi legati ad un utilizzo non corretto di internet.;
- c) Organizzazione di uno o più incontri formativi nel corso dell'anno scolastico sulle dinamiche che si possono instaurare fra i pari con l'uso di cellulari e smartphone o delle chat o social-network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo;
- d) Nel Patto di Corresponsabilità Educativa sottoscritto dai docenti e dai genitori a inizio del percorso scolastico, aggiunta di una voce specifica sul tema dell'utilizzo consapevole e sicuro di internet e delle tecnologie digitali;
- e) Ricerca di collaborazione tra docenti e genitori nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali.

2.4. Gli strumenti TIC a supporto dell'inclusione e partecipazione

Le TIC sono oramai parte integrante della vita quotidiana degli studenti, con un impatto su molti aspetti della società, tra cui la scuola. Il potenziale di questi strumenti può contribuire a ridurre l'esclusione sociale e aumentare la partecipazione di ogni studente con la sua particolarità.

Bisogna ricordare, però, che Internet veicola molti stereotipi (di genere, razziali, culturali, sessuali, etc.), i quali, tuttavia, possono essere combattuti a scuola.

Per inclusione, pertanto, s'intende un concetto ampio, che comprende la non discriminazione (art. 2 della Convenzione ONU sui diritti dell'infanzia e dell'adolescenza). L'obiettivo è far sentire ogni studente membro attivo della comunità scolastica, ed è raggiungibile solo se condiviso non solo dal personale della scuola, ma da ogni studente e dalla comunità scolastica allargata.

Il PC ed ogni apparecchio tecnologico sono strumenti fondamentali anche per lo sviluppo delle conoscenze e delle capacità dei diversamente abili e degli alunni con difficoltà cognitive e relazionali, perché favoriscono non solo la loro integrazione all'interno della classe, ma suscitano in essi una grande autostima.

La capacità di poter fare ciò che fanno i compagni ed il poterlo fare con questi strumenti compensativi, non li esclude “dal gioco”, anzi li rinforza e li rende “fortemente abili”. Il computer dà la possibilità a questi studenti anche di un apprendimento collaborativo che può prevedere uno scambio di informazioni (vedi le ricerche in Internet) e di competenze informatiche, facendogli acquisire un giusto grado di autonomia nel lavoro.

Nei casi di discalculia poi, cioè di compromissione delle capacità di calcolo, il computer offre la possibilità di svolgere esercizi in autonomia, con l’autocontrollo dei risultati, con ritmi e frequenze personalizzati, con difficoltà graduali rispetto all’alunno; anche il procedimento per arrivare alla soluzione può essere incanalato perché più utile a risolvere una specifica situazione problematica. L’ambiente informatico rende concreti problemi e operazioni che negli esercizi su carta appaiono allo studente molto astratte.

Dunque, l’utilizzo delle Tecnologie dell’Informazione e della Comunicazione (TIC) nei contesti di apprendimento, consente molteplici possibilità di adattamento delle attività e, nei diversamente abili o certificati B.E.S., promuove la motivazione, la partecipazione e l’interazione con gli altri; le TIC aiutano inoltre a mantenere l’attenzione e favoriscono lo sviluppo dell’autostima.

Allo stesso modo, un’adeguata formazione degli insegnanti è un requisito fondamentale in tutto il processo.

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

3.1. Accesso a internet

L'Istituto Comprensivo, nella fase conclusiva dell'anno scolastico 2016-2017, ha in funzione tre plessi (Primaria e Secondaria Via De Finetti, misto di Via Capelli), tutti dotati di accesso ad internet e di diffusione interna della connessione sia mediante rete fisica, sia mediante Wi-Fi. L'I. C., inoltre, ha appena avuto in consegna due nuovi plessi in Via Brunetti (destinati alla scuola secondaria e alla scuola dell'infanzia) che dovranno entrare in funzione dall'anno scolastico 2017-2018 ed essere quindi dotati di connettività.

A causa di limiti infrastrutturali del quartiere in cui l'Istituto è ubicato, di recente sviluppo, gli accessi ad internet dei tre plessi scolastici hanno un'ampiezza di banda limitata, dell'ordine di 7 Mbit/s per plesso (inferiore all'ampiezza di molte connessioni domestiche). L'evoluzione infrastrutturale del quartiere è comunque monitorata al fine di poter dotare i plessi di una connettività più adatta alle dimensioni dell'Istituto.

In merito alla dotazione strumentale, sono dotate di Lavagna Interattiva Multimediale tutte le aule del plesso della scuola secondaria di Via De Finetti, 5 aule del plesso della Primaria, sempre di Via De Finetti, e 6 aule del plesso di Via Capelli. Le LIM sono collegate a computer fissi o portatili, eterogenei anche per caratteristiche ed età. Inoltre, i tre plessi sono dotati di laboratori informatici di diversa capienza: 13 postazioni quello del plesso di Via Capelli, 15 postazioni quello della Primaria a Via De Finetti, 20 postazioni quello della Secondaria a Via De Finetti. Quest'ultimo è stato recentemente realizzato utilizzando la donazione, da parte di un'azienda, di 20 PC usati con almeno 5 anni di vita, e quindi con un'operatività parzialmente limitata.

Per le attività extra aula i docenti hanno a disposizione uno o due computer per plesso.

Ogni plesso è dotato di un server, con sistema operativo Zentyal che integra la funzione di proxy server con filtraggio della navigazione sul web mediante gestione di blacklist ed eccezioni. Le impostazioni sono definite dal referente tecnologico, con l'approvazione del Dirigente Scolastico, e applicate con il supporto dei tecnici della società esterna fornitrice di assistenza informatica.

È in carico a ciascun docente la segnalazione di malfunzionamenti e disservizi eventualmente riscontrati.

3.2. Gestione accessi

Nei computer presenti nelle aule, nei laboratori e nelle sale docenti non sono attualmente sempre presenti più profili di accesso. Alle postazioni docente nelle aule, generalmente, si accede ad un unico profilo inserendo una password uguale per tutti; solo alcuni computer di recente installazione, destinati a postazioni docente nelle aule, dispongono di un doppio profilo di accesso amministratore / utente.

Non è previsto un backup automatico su server e non è al momento attiva una politica di backup.

Le disposizioni organizzative in merito all'utilizzo della rete e degli strumenti informatici specificano, per il personale docente, la regola di poter creare all'interno della cartella 'Documenti' dei computer a propria disposizione una cartella personale (nominata con il proprio cognome) in cui salvare solo una copia dei propri file lavorativi, non l'esemplare unico.

La scarsa ampiezza della banda disponibile ha influenzato alcune scelte relative alla possibilità di fruizione della connettività: attualmente, infatti, a docenti, alunni e utenti esterni non è consentito l'accesso al Wi-Fi dai propri dispositivi personali.

I tecnici dell'assistenza informatica esterna e i referenti tecnologici di plesso sono a conoscenza delle password per accedere al Wi-Fi e al server.

3.3. E-mail

L'Istituto non ha ritenuto necessario fornire al proprio personale un account di posta elettronica sul dominio del proprio indirizzo web, con l'eccezione del Dirigente Scolastico che dispone di una casella di tale tipo.

L'account istituzionale generale (codicemeccanografico@istruzione.it) è utilizzato ordinariamente dagli uffici amministrativi e si dispone di una casella istituzionale di posta elettronica certificata.

I docenti possono utilizzare per scopi didattici i propri account personali che possono essere collegati al proprio profilo del Registro Elettronico Axios, in modo da ricevere notifiche e comunicare con i familiari degli alunni senza far conoscere il proprio indirizzo.

3.4. Sito web della scuola

L'Istituto ha un sito web aggiornato direttamente dal Dirigente Scolastico e dal Direttore servizi generali e amministrativi, che sono quindi responsabili dell'accuratezza e dell'appropriatezza del contenuto inserito.

In una logica di trasparenza il sito consente al pubblico di accedere ad una grande quantità di informazioni e documenti, sia nelle sezioni istituzionali, sia in quelle specifiche riservate ai rapporti scuola-famiglia.

Il sito dispone di un'area riservata per i docenti che consente di accedere, mediante un'unica password uguale per tutti, alle circolari e alla modulistica.

Il sito dispone di un'area riservata per il personale ATA e di una per i docenti, che consente di accedere, mediante un'unica password uguale per tutti, alle circolari e alla modulistica.

Da poco è attiva anche, in via sperimentale, una bacheca virtuale che consente di condividere contenuti tra alunni, genitori e docenti. I contenuti necessitano di approvazione da parte dell'amministratore della bacheca (Animatore digitale) per essere pubblicati.

3.5. Social network

Attualmente la configurazione dei proxy server non consente dalla rete scolastica l'accesso ai siti di social networking e l'utilizzo di questi ultimi non è integrato sistematicamente nelle pratiche didattiche.

Uno degli obiettivi futuri è quello di educare gli studenti ad un uso consapevole, responsabile e sicuro degli stessi, anche al di fuori del contesto scolastico, informando e sensibilizzando in tal senso le famiglie e il corpo docente. In questo ambito è possibile prevedere l'accesso per un'iniziativa specifica, previa

autorizzazione del Dirigente Scolastico.

Da pochi mesi, invece, è attivo, in chiave sperimentale, l'accesso al portale web YouTube, esclusivamente per l'utilizzo didattico, da parte dei docenti, di video brevi che abbiano carattere formativo e non di intrattenimento. Ciò nella consapevolezza che, a causa della scarsa ampiezza di banda, l'utilizzo simultaneo di video in streaming da parte di diversi utenti rischia di causare il rallentamento o il blocco della rete, inibendone anche le funzioni primarie, come il Registro Elettronico. Ai docenti, infatti, è oggi consigliato di scaricare preventivamente i video da YouTube e utilizzarli in aula in versione offline, anche seguendo una logica di preparazione preventiva delle attività didattiche.

Relativamente, infine, all'uso personale dei social network e dei sistemi di messaggistica istantanea (tipo Whatsapp) anche al di fuori del contesto scolastico, da parte del personale non docente e docente, è raccomandato soprattutto a quest'ultimo di non stabilire connessioni amicali con gli alunni e i loro familiari al fine di evitare canali di comunicazione troppo diretti e l'accesso ad informazioni personali che potrebbero essere utilizzate impropriamente.

3.6. Protezione dei dati personali

Per la protezione dei dati personali si fa riferimento a tutto quanto previsto dal Decreto legislativo n. 196 del 30 giugno 2003 (c. d. Codice della Privacy).

Il Dirigente Scolastico è titolare del trattamento dei dati personali e il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori etc.) nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione.

In aggiunta, si ritiene utile individuare al riguardo alcune linee guida di e-safety:

- All'atto dell'iscrizione è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico di immagini e video dei minori.
- Le fotografie e/o i video da pubblicare eventualmente su internet, che includano allievi, sono selezionati con cura e non permettono a singoli di essere chiaramente identificati a meno che non si tratti di eventi particolari per cui le famiglie possono concedere opportuna autorizzazione. Si preferisce l'utilizzo di fotografie di gruppo piuttosto che di foto riconoscibili di singoli.
- È vietato pubblicare i nomi completi degli alunni sul sito web istituzionale, come pure in eventuali altri siti, blog, forum, social e wiki.
- Ogni caso particolare è preso in considerazione per stabilire l'opportunità di pubblicare dati personali ed eventualmente è presentata apposita richiesta circostanziata che vale solo per lo specifico evento.
- Il personale non deve in nessun caso lasciare sui dispositivi hardware scolastici di uso comune file o materiale contenente dati personali propri, degli alunni, dei familiari etc.
- Al personale è sconsigliato condividere numeri di telefono personali o indirizzi di posta elettronica privati con la componente studentesca e con i genitori, fatta eccezione per i rappresentanti di classe, che è bene valorizzare come collettori di comunicazione rispetto alle altre

famiglie. È opportuno indirizzare la comunicazione verso i colloqui in presenza durante l'orario di ricevimento, utilizzare il più possibile le funzionalità comunicative del Registro Elettronico e fornire, all'occorrenza, il recapito telefonico dell'Istituto.

3.7. Gestione e utilizzo dei laboratori informatici

I laboratori informatici sono costituiti da aule provviste di LIM e da postazioni PC numerate e messe in rete con connessione internet tramite rete LAN. Con i PC in dotazione è possibile utilizzare CD e dispositivi USB.

All'interno del laboratorio è presente la seguente documentazione:

- Regolamento
- Registro firme e segnalazioni.

Sulla porta d'ingresso è affisso il modulo con l'orario settimanale dove registrare le prenotazioni.

Il laboratorio, quando non in uso, è chiuso con una chiave che viene custodita dalla collaboratrice scolastica che presidia il piano.

Norme di Comportamento (es. laboratorio Secondaria De Finetti)

1. Il laboratorio è a disposizione di tutte le classi dal lunedì al venerdì, dalle ore 8.15 alle ore 14.15
2. L'accesso al laboratorio è regolamentato da un orario settimanale prestabilito e va prenotato dal docente almeno un giorno prima.
3. Non è consentito prenotare il laboratorio per più di due ore giornaliere consecutive.
4. Il docente, visto il quadro orario programmato, può accedere al laboratorio, con la classe o gruppi di alunni, nelle ore non occupate, per svolgere le attività didattiche. Se si verificano troppe richieste d'uso, i docenti interessati cercheranno serenamente un accordo rispettando il principio che tutti gli insegnanti, di qualsiasi disciplina, hanno lo stesso diritto di usare le strumentazioni per finalità didattiche.
5. Il docente ha il dovere compilare dettagliatamente e in ogni parte il registro posto all'interno del laboratorio, sul quale devono essere annotati la classe, l'insegnante accompagnatore, l'orario e le eventuali problematiche riscontrate.
6. Nei laboratori non è consentito consumare pasti di alcun tipo. Nell'eventualità della coincidenza con la ricreazione gli alunni sono obbligati a uscire dall'aula, consumare la propria merenda e rientrare a ricreazione ultimata.
7. All'uscita il docente e gli alunni devono risistemare i PC (spegnendoli se non vi è un nuovo gruppo che subentra), le sedie, i tavoli e quant'altro e controllare che non vi siano cartacce o rifiuti.
8. Gli alunni non devono mai essere lasciati ad operare da soli, senza la supervisione del docente accompagnatore.
9. Nell'utilizzo del PC i docenti possono salvare copia dei propri file solo in cartelle personali, identificate dal proprio cognome e nome, da creare all'interno della cartella 'DOCUMENTI' e non sul desktop. Sui PC delle postazioni i file possono essere copiati solo temporaneamente, durante la sessione di lavori, e devono essere rimossi al termine (utilizzando dispositivi di archiviazione mobile come

pennette usb etc.) Periodicamente tutti i PC della rete vengono controllati e ripuliti, tutti i file memorizzati fuori dalle rispettive cartelle saranno cancellati. I docenti, a fine anno, devono cancellare i propri file e cartelle per alleggerire la memoria dei computer e favorire la manutenzione straordinaria dei sistemi operativi.

10. L'accesso alla rete Internet è consentito esclusivamente per uso didattico. Gli utenti sono tenuti a rispettare le regole specifiche relative all'uso della rete. I docenti sono tenuti a vigilare su eventuali usi impropri della rete da parte degli alunni.
11. I docenti sono tenuti a garantire il corretto utilizzo delle apparecchiature e dei materiali e ad usarli in modo da evitare qualsiasi danneggiamento.
12. Il personale e gli allievi devono rispettare le procedure corrette di accensione, utilizzo e spegnimento delle macchine (non togliere mai la corrente fino a quando i computer non hanno terminato la fase di spegnimento). Quando le lezioni nel laboratorio sono consecutive è compito degli ultimi utenti spegnere le apparecchiature.
13. Non è consentito portare via dal laboratorio materiale di alcun tipo.
14. Non è consentito installare alcun tipo di software aggiuntivo su qualsiasi macchina senza preventiva autorizzazione da parte del referente del laboratorio.
15. Ogni evenienza, situazione anomala, irregolarità rispetto al presente regolamento, nonché eventuale malfunzionamento dell'attrezzatura in dotazione, va segnalata tempestivamente al referente del laboratorio e annotata nell'apposito registro.

4. Strumentazione personale

4.1. Per gli studenti

Il regolamento d'Istituto, recependo le linee di indirizzo del MIUR in materia di utilizzo di telefoni cellulari ed altri dispositivi elettronici (C.M. n. 30/2007), vieta l'uso dei suddetti dispositivi durante tutta l'attività scolastica (comprese la mensa, l'interscuola e le attività extracurricolari).

In caso di urgenza, per comunicazioni tra gli alunni e le famiglie, su autorizzazione dei docenti e sotto il diretto controllo dei collaboratori scolastici, è consentito l'uso del telefono della scuola per comunicare eventuali stati di malessere o per altri motivi di effettiva necessità.

È fatto esplicito divieto dell'uso di smartphone e di tutti gli apparecchi elettronici in grado di fotografare e filmare. La materia è regolata dalla normativa sulla privacy (v. Dir. MIUR n. 104/2007).

Durante le uscite didattiche ed i viaggi d'istruzione è consentito l'uso di telefoni cellulari e smartphone per ascoltare musica, effettuare fotografie e riprese video attinenti l'uscita e solo previa autorizzazione del docente accompagnatore. Le fotografie e/o i video non potranno comunque essere pubblicati su qualsiasi sito internet e/o diffusi tramite sistemi di messaggistica senza l'esplicita autorizzazione dei genitori dei minori ripresi.

In caso di attività didattiche espressamente programmate dai docenti che prevedano l'utilizzo di strumenti personali quali smartphone, tablet, computer portatili, video-fotocamere, registratori vocali etc., ciò potrà avvenire, in deroga al regolamento, sotto la stretta supervisione del docente responsabile e solo per la durata dell'attività didattica.

Individui con disabilità e/o con disturbi specifici di apprendimento, previa consultazione con il Consiglio di Classe, possono concordare le modalità di impiego di alcuni dei suddetti dispositivi elettronici quali strumenti compensativi.

In ogni caso non possono essere portati a scuola dispositivi elettronici espressamente dedicati all'intrattenimento, quali giochi e console, che peraltro possono avere un accesso ad internet non filtrato.

Infine, si raccomanda vivamente di non inviare e diffondere, dai propri dispositivi personali, materiali abusivi, potenzialmente offensivi o inappropriati, anche all'interno di cerchie o gruppi di discussione privati e al di fuori dell'orario scolastico.

4.2. Per i docenti e tutto il personale della scuola

Il regolamento d'Istituto estende il divieto di utilizzare telefoni cellulari durante lo svolgimento dell'attività di insegnamento-apprendimento anche nei confronti del personale docente e ATA (C.M. n. 362/1998).

Tuttavia, vista l'ampia gamma di usi possibili associati a dispositivi personali, quali smartphone e tablet (agenda, task-list, risorse digitali quali e-book etc.), l'utilizzo di tali dispositivi è consentito sia per funzioni di organizzazione personale funzionali allo svolgimento del proprio servizio, sia per scopo didattico (da parte dei docenti), ad integrazione dei dispositivi scolastici disponibili (per esempio per l'utilizzo del Registro Elettronico).

L'uso, invece, finalizzato alla comunicazione, dei cellulari (chiamate vocali e messaggistica), durante l'orario di servizio, è consentito al personale solo in casi di urgenza e per il personale docente non può costituire fonte di interruzioni o distrazioni dall'attività didattica.

5. Prevenzione, rilevazione e gestione dei casi

5.1. Prevenzione

Rischi

Da alcuni anni ormai l'apporto delle nuove tecnologie ha rivoluzionato il nostro modo di vivere e di relazionarci. La scuola, in qualità di principale istituzione educativa, è chiamata a guidare le nuove generazioni di studenti in questo cambiamento epocale con l'obiettivo di far scaturire in loro un atteggiamento mentale e culturale che li porti a considerare le grandi potenzialità degli strumenti digitali ma al contempo i numerosi rischi insiti in un uso scorretto degli stessi. Una buona prevenzione e educazione all'utilizzo delle TIC permette a chiunque fruisca della Rete non soltanto di evitare situazioni di rischio, bensì di padroneggiare gli strumenti giusti per affrontarle nel momento in cui queste si presentano.

Diversi sono i comportamenti online che possono richiedere alla scuola un approfondimento e una eventuale segnalazione, tra i quali quelli che fanno riferimento a:

- contenuti e atteggiamenti aggressivi e violenti (cyberbullismo, messaggi minacciosi, offensivi e violenti, informazioni false, immagini e video umilianti, contenuti xenofobi,);
- pedopornografia online, o più in generale immagini e video a sfondo sessuale;
- violazione della privacy (invio e scambio di informazioni, foto, video, immagini private e riservate);
- dipendenze di diverse tipo.

Azioni

L'Istituto IC "Via De Finetti" ritiene indispensabile elaborare strategie efficaci di contrasto e prevenzione alle più diverse forme di rischio cui oggi sono esposti i nostri studenti che navigano sul Web. Partendo anche dai bisogni che emergono presso gli alunni stessi, si potranno approfondire le tematiche di maggiore interesse attraverso attività didattiche mirate (unità di apprendimento da realizzare nelle diverse discipline, iniziative, approfondimenti) o momenti più o meno formali in cui avviare discussioni guidate e confronti con la classe o con gruppi più allargati. A titolo di esempio, per prevenire casi di cyberbullismo, il docente può agire monitorando costantemente le relazioni interne alla classe per individuare eventuali situazioni di disagio e indirizzare il gruppo verso un clima di positiva accettazione e di rispetto l'uno dell'altro.

Le iniziative dei docenti saranno necessariamente supportate da esperti esterni, attraverso, ad esempio, la partecipazione della scuola a progetti e/o iniziative coerenti con i temi del digitale, organizzati da Enti e/o Associazioni di comprovata affidabilità. Le tecnologie digitali sono, per loro natura, in perenne cambiamento e aggiornamento, di conseguenza anche gli adulti dell'intera comunità educante sono chiamati a essere costantemente formati su queste tematiche al fine di poter fronteggiare in maniera adeguata e competente le diverse problematiche che possono sorgere presso bambini e adolescenti.

Dal canto suo, anche la famiglia è pienamente coinvolta in questo processo in quanto è chiamata a educare i propri figli, ma anche a vigilare sui loro comportamenti. Il coinvolgimento dei genitori è quindi previsto sia nella fase della prevenzione, attraverso la partecipazione a incontri e eventi di informazione e

sensibilizzazione, sia in quella di rilevazione e gestione dei casi. Alla famiglia spetta, ad esempio, di attivare forme di controllo parentale della navigazione sul Web e monitorare l'esperienza online dei propri figli. I genitori stessi inoltre sono invitati a proporre alla scuola tematiche sulle quali focalizzare un possibile intervento di studio e approfondimento.

In un'ottica di prevenzione del disagio giovanile e di gestione dei comportamenti online a rischio l'Istituto Comprensivo "Via De Finetti" intende attivare per l'anno scolastico 2017/2018 uno sportello d'ascolto. L'adolescenza è una fase di vita molto complessa e delicata, durante la quale i ragazzi cominciano a definire le proprie scelte personali e si impegnano in un processo di costruzione dell'identità.

La scuola secondaria di primo grado riveste, in questa fase, un'importanza cruciale sia per i ragazzi che per le famiglie, non solo per la formazione didattica educativa, ma anche come luogo di riferimento nel quale si strutturano le relazioni con il gruppo dei pari, che assume in questi anni un ruolo centrale.

I cambiamenti che l'adolescente si trova ad affrontare sono molteplici e incalzanti: rapide trasformazioni del corpo, sviluppo delle capacità cognitive e una maggiore capacità di riflessione su di sé e sull'altro, ricerca dell'autonomia. Questi processi, talvolta, se non accompagnati da un'adeguata riflessione, possono portare l'adolescente a esperire disagio e confusione. Per questi motivi, la nostra Scuola si impegna per creare un clima favorevole all'accoglienza, basato sulla fiducia, sul rispetto delle diversità, sulle capacità comunicative, relazionali e creative di ciascuno, promuovendo non solo l'inserimento e l'integrazione di tutti gli alunni ma anche preoccupandosi di costruire un ambiente funzionale all'apprendimento e allo stare bene insieme, un ambiente nel quale ha un ruolo fondamentale lo spazio aperto all'ascolto attivo. Tra le misure di prevenzione che la scuola mette in atto ci sono, altresì, azioni finalizzate a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle diversità così che l'utilizzo di Internet e dei cellulari oltre che collocarci all'interno di un sistema di relazioni, ci renda consapevoli di gestire con un certo grado di lucidità i rapporti che si sviluppano in tale ambiente, giungendo a riconoscere e gestire le proprie emozioni.

5.2. Rilevazione

-Che cosa segnalare

La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti e contesti. Tutti gli adulti presenti nella scuola sono invitati a essere custodi diretti o indiretti di situazioni problematiche vissute e devono poter accogliere le confidenze o le richieste di aiuto degli alunni rispetto a situazioni di disagio vissute. Il docente, il personale ATA e le altre figure educative che affiancano gli insegnanti, possono venire a conoscenza di situazioni problematiche in diversi modi: eventi osservati direttamente in classe e/o a scuola, fatti confidati dall'alunno coinvolto oppure riferiti da terzi.

-Come segnalare: quali strumenti e a chi

Una volta effettuata la rilevazione, il docente compila un "Modulo di segnalazione" (vedi allegato) e contatta il Referente individuato in ciascun plesso per condividere quanto avvenuto.

Quest'ultimo, a seconda del fatto accaduto, può decidere di rivolgersi al Dirigente Scolastico.

Nei casi di particolare gravità, ovvero quando l'episodio si configura come una fattispecie di reato, sarà necessario valutare con il Dirigente Scolastico un'eventuale segnalazione alle autorità competenti (Forze

dell'Ordine; Polizia Postale e della Comunicazioni). Laddove vi siano implicazioni sul piano sociale e psicologico ci si potrà rivolgere ai servizi sociali.

Come precedentemente detto, le famiglie degli alunni coinvolti, sia in qualità di vittime sia di responsabili della condotta scorretta, saranno tempestivamente messe a conoscenza dell'accaduto.

In particolare, a seconda dell'entità dei fatti si provvederà:

- a una comunicazione scritta sul diario
- a una nota disciplinare sul Registro di Classe
- a una convocazione formale dei genitori degli alunni, tramite segreteria;
- a una convocazione delle famiglie da parte del Dirigente Scolastico.

-Come gestire le segnalazioni

Gli insegnanti, anche con l'ausilio del personale di assistenza tecnica, possono tenere traccia delle prove del comportamento da segnalare se si tratta di condotte scorrette o di abusi rilevati sulla strumentazione in uso nella scuola. Al contrario, il docente non può intervenire direttamente sui telefoni cellulari di proprietà degli alunni senza l'esplicita autorizzazione dei genitori. Ciononostante si può chiedere allo studente di conservare tutto ciò che possa tornare utile per l'individuazione del fatto accaduto e di chi l'ha compiuto (messaggio, voce, testo, immagine, numero di cellulare) sia nel caso in cui egli sia la vittima, sia nel caso in cui un alunno non coinvolto direttamente venga a conoscenza di abusi e condotte lesive subite da compagni. Qualora non si disponga di prove, ma solo di testimonianze riferite a voce, le informazioni vengono comunque raccolte dai docenti al fine di avviare la procedura precedentemente delineata.

Si prevede la possibilità di compilare un *diario di bordo* per tenere traccia del caso segnalato, delle azioni intraprese dalla scuola e delle conseguenze scaturite dall'intervento posto in essere. A lungo termine questo strumento di monitoraggio favorisce la raccolta delle pratiche operative messe in atto e può costruire una memoria condivisa della scuola.

5.3 Gestione dei casi

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

Le procedure interne per la rilevazione e gestione dei casi avvengono secondo i protocolli suggeriti dalla piattaforma "Generazioni Connesse".

Al fine di supportare la scuola nella gestione di situazioni problematiche, il Safer Internet Centre mette a disposizione sia per adulti che per minorenni la possibilità di contattare la linea gratuita di ascolto 1.96.96 di *Telefono Azzurro* (attiva 24 ore su 24, 365 giorni l'anno) e la chat (www.azzurro.it/chat; gratuita e attiva dal lunedì al venerdì dalle 8 alle 22 e il sabato/domenica dalle 8 alle 20) gestite da operatori e esperti preparati sulle tematiche inerenti l'utilizzo dei nuovi media.

Altri servizi utili sono le due Hotline gestite rispettivamente da *SOS Il Telefono Azzurro Onlus* (www.azzurro.it/clicca-e-segnala) e da *Save The Children* (www.stop-it.it). Entrambe offrono un servizio di segnalazione, attraverso un modulo online, di materiale pedopornografico o potenzialmente dannoso per chi naviga sul Web.

La Polizia Postale e delle Comunicazioni si occupa di accogliere tutte le segnalazioni o denunce relative a reati di tipo informatico (furto di identità, cyberbullismo, commercio on-line con clonazione di carte di credito, pedopornografia on-line, grooming, gioco d'azzardo on-line, sexting).

Il Policlinico Gemelli di Roma ha attivato un ambulatorio che prevede un trattamento integrato per le dipendenze da Internet e i casi di cyberbullismo.

La gestione dei casi rilevati va differenziata a seconda della gravità: alcuni episodi minori potranno per esempio essere affrontati e risolti con la discussione collettiva in classe e la pianificazione di un intervento educativo adeguato; altri gestiti attraverso un colloquio informale con l'allievo/a interessato/a e i genitori dello stesso con la finalità di analizzare e riflettere su quanto avvenuto e avviare un percorso condiviso di sostegno.

E' bene in tutti i casi condividere a livello di Consiglio di Classe ogni episodio rilevato, sia esso anche di minima entità.

Nella tabella seguente viene elencata la principale casistica che può scaturire da una navigazione non corretta sul Web e le possibili azioni da intraprendere come risposta.

CASO	AZIONE
<p>CYBERBULLISMO</p> <p>Si tratta di una forma di prevaricazione mirata a danneggiare una persona o un gruppo, ripetuta nel tempo e perpetuata da una persona o un gruppo di persone "più potenti" nei confronti di un'altra percepita come "più debole".</p> <p>Il cyberbullismo viene attuato attraverso l'utilizzo delle Tecnologie per l'Informazione e la Comunicazione (social network, chat, email, blog, forum, siti di foto-video sharing, ecc.) e può esplicarsi in particolare nei seguenti modi:</p> <ul style="list-style-type: none"> -invio di sms, messaggi in chat, e-mail offensive o di minaccia -diffusione di messaggi offensivi ai danni della vittima, divulgando sms o e-mail nelle mailing list o nelle chat-line -pubblicazioni nel cyberspazio di foto o filmati che ritraggono atti di prepotenza e denigrazione nei confronti della vittima <p>Due elementi utili a effettuare una valutazione di questa fattispecie di comportamento sono: la modalità in cui avvengono (presenza di un pubblico? Comportamento reiterato? Comportamento intenzionale? Tra coetanei?) l'età dei protagonisti (il reato di bullismo è previsto per i soli minorenni). Sarà da valutare l'eventuale stato di disagio vissuto dalla persona coinvolta.</p>	<p>La casistica può essere molto varia. In linea generale questa la procedura da attuare:</p> <ul style="list-style-type: none"> - comunicazione alla famiglia - comunicazione al consiglio di classe - intervento sull'intero gruppo classe, al fine di negoziare e risolvere situazioni di conflitto, di prevaricazione, di sofferenza. <p>Se ci si trova di fronte a una fattispecie di reato (furto di identità, condotta persecutoria che mette a rischio il benessere del bambino coinvolto) ci si può rivolgere a:</p> <ul style="list-style-type: none"> -Polizia di Stato – Compartimento di Polizia Postale e delle Comunicazioni -Polizia di Stato – Questura o Commissariato di P.S. del territorio -Arma dei Carabinieri – Comando Provinciale o Stazione del territorio <p>Le richieste di aiuto di giovani vittime di cyberbullismo potranno essere prese in carico da Telefono Azzurro al numero 19696; potrebbe essere necessario anche rivolgersi a un servizio territoriale di supporto psicologico e/o di mediazione.</p>
<p>SEXTING</p> <p>Si tratta dello scambio di immagini o video che ritraggono persone minorenni nude, seminude o</p>	<p>Prevenzione: sensibilizzazione sul tema anche con l'ausilio di progetti e realtà esterni.</p>

<p>in atteggiamenti sessuali. Diversi sono gli aspetti critici implicati:</p> <ul style="list-style-type: none"> -controllo: una volta caricato sul Web del materiale di questo genere, remote sono le possibilità di eliminarlo in modo definitivo; -la reputazione: immagini di questo genere ledono la reputazione di chi vi è ritratto; -adescamento da parte di adulti potenziali abusanti; -pedopornografia: sono immagini che rientrano nella definizione di materiale pedopornografico. <p>Produrre e diffondere questo materiale è reato.</p>	<p>È urgente:</p> <ul style="list-style-type: none"> -rivolgersi al più vicino Compartimento di Polizia Postale e delle Comunicazioni per richiedere la rimozione del materiale, per quanto possibile, se online, e il blocco della sua diffusione sui dispositivi mobili.
<p>GROOMING (Adescamento online) È l'adescamento sessuale online di minori. Gli adulti entrano in contatto con bambini e/o adolescenti attraverso i diversi strumenti della Rete e progressivamente ne conquistano la fiducia, fino a rendere il loro rapporto esclusivo. Sia maschi che femmine sono esposti a casi di grooming.</p>	<p>Prevenzione: è bene far conoscere agli alunni la possibilità che adulti malintenzionati si propongano loro su Internet con finalità intenzionalmente malevoli.</p> <p>In caso di sospetti occorre:</p> <ul style="list-style-type: none"> -non toccare più il PC utilizzato dal minorenne -rivolgersi alle autorità competenti -rivolgersi ai servizi socio-sanitari del territorio di appartenenza.
<p>DIPENDENZA DA INTERNET È l'utilizzo eccessivo e incontrollato di Internet. Può subentrare un comportamento patologico quando si palesa:</p> <ul style="list-style-type: none"> -un uso eccessivo, con perdita del senso del tempo -senso di straniamento con sentimenti di rabbia e tensione quando PC e Rete sono inaccessibili -ripercussioni negative sia nell'ambito scolastico che sociale- discussioni, bugie, isolamento sociale. 	<p>Se si ravvisa un rischio per il benessere psicofisico delle persone minorenni ci si può rivolgere:</p> <ul style="list-style-type: none"> - al pediatra o medico di base, in una fase iniziale, -ai servizi socio-sanitari del territorio di appartenenza (consultori familiari, servizi di Neuropsichiatria Infantile, centri specializzati sulle dipendenze, etc...).
<p>VIDEOGIOCHI ONLINE Il rischio consiste nell'uso eccessivo dei videogiochi, in particolare se:</p> <ul style="list-style-type: none"> -si trascurano altre attività sociali e la scuola; -c'è una caduta nel rendimento scolastico -il ragazzo tende a essere apatico e/o irascibile quando non gioca. 	<p>Un'eventuale azione può essere intrapresa quando è messo in pericolo il benessere psicofisico della persona.</p>
<p>GIOCO D'AZZARDO ONLINE Consiste nello scommettere denaro o altri beni sull'esito futuro di un evento tramite un sito web. I giochi d'azzardo online prevedono la vincita o la perdita di somme di denaro reale.</p>	<p>Qualora sia rilevato l'uso di un gioco d'azzardo in Rete da parte di minorenni ci si può rivolgere a:</p>

<p>Il gioco d'azzardo è vietato ai minorenni.</p>	<p>-Compartimento di Polizia Postale e delle Comunicazioni per segnalare l'accessibilità dei siti che gestiscono i giochi; -Servizi e strutture specializzate del territorio se si tratta di un caso patologico di dipendenza da Internet.</p>
<p>SITI PRO-SUICIDIO Sono siti che nel cyber spazio promuovono, orientano o motivano a condotte autolesive. Rappresentano un serio pericolo per gli adolescenti.</p>	<p>A seconda del livello di rischio ci si potrà rivolgere a: -Polizia Postale e delle Comunicazioni; -Strutture pubbliche preposte a offrire una consultazione generica o specifica (pediatra; Consultorio Familiare, servizio di Neuropsichiatria) per supporto socio-sanitario.</p>
<p>SITI PRO-ANORESSIA Sono spazi virtuali (blog, forum, profili sui social network) in cui vengono diffusi consigli e tecniche mirate a contrastare la fame e promuovere l'assunzione di comportamenti alimentari disfunzionali.</p>	<p>È opportuno rivolgersi a: -strutture preposte ad offrire il necessario supporto psicologico e/o sanitaria; -eventuali strutture specializzate nella valutazione e trattamento dei disturbi alimentari.</p>
<p>PEDO-PORNOGRAFIA ONLINE È un reato che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti persone minorenni coinvolte in comportamenti sessualmente espliciti, concrete o simulate o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali. La Rete ha notevolmente contribuito alla produzione e diffusione di questo materiale.</p>	<p>Se vi sono persone minorenni coinvolte nella visione e/o produzione di questo materiale sarà opportuno rivolgersi ai servizi socio-sanitari del territorio di appartenenza. Qualora navigando in rete si trovi materiale pedopornografico è opportuno segnalarlo anche in forma anonima sul sito "Generazioni connesse" nella sezione Hotline.</p>