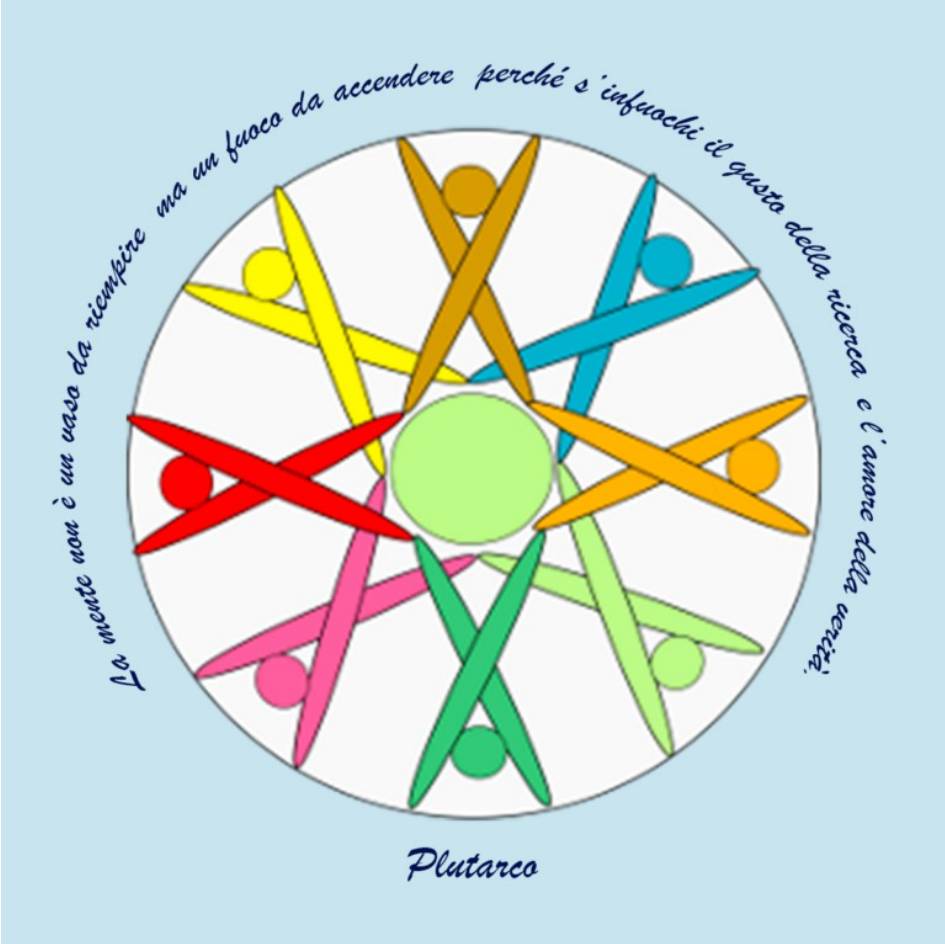
ISTITUTO COMPRENSIVO DI CUCCIAGO CASNATE GRANDATE

ANNO SCOLASTICO 2025/2026



E-SAFETY POLICY

INDICE

1. INTRODUZIONE

1.1 Premessa

1.2 Scopo della Policy

1.3 Ruoli e Responsabilità

1.3a) Ruolo della scuola nel contrasto al cyberbullismo

1.3b) Ruolo della Comunità scolastica nel rispetto della E-Policy

1.4 Condivisione e comunicazione della Policy all'intera comunità scolastica

1.5 Gestione delle infrazioni alla Policy

1.6 Procedure operative per la gestione delle infrazioni alla Policy

1.6a) Che cosa segnalare

1.6b) Come segnalare e a chi

1.6c) Come gestire le segnalazioni

1.7 Monitoraggio dell'implementazione della Policy e suo aggiornamento

1.8 Integrazione della Policy con Regolamenti esistenti

2. FORMAZIONE E CURRICOLO

2.1 Curricolo sulle competenze digitali per gli studenti

2.2 Formazione dei docenti

2.3 Sensibilizzazione delle famiglie

3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA

3.1 – Protezione delle strumentazioni e della navigazione

3.2 Gestione accessi

3.2a) Accesso alle strumentazioni scolastiche

3.2b) Accesso alla rete scolastica

3.2c) Accesso ad Internet

3.3 Email

3.4 Sito web della scuola

3.5 Social network

3.6 – Registro scolastico

3.6a) Area Amministrativa
3.6b) Area Docenti
3.6c) Area esercenti responsabilità genitoriali

3.7 Protezione dei dati personali

3.7a) Procedure operative per la protezione dei dati personali

4. STRUMENTAZIONE PERSONALE

4.1 Studenti

4.2 Docenti

4.3 Personale amministrativo e collaboratori scolastici

4.4 Altri operatori

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

5.1 Prevenzione

5.1a) Rischi
5.1b) Azioni per la riduzione dei rischi

5.2 Rilevazione

5.2a) Che cosa segnalare

5.2b) Come segnalare e a chi

5.2c) Come gestire le segnalazioni

5.3 Gestione dei casi

5.3a) Definizione delle azioni da intraprendere a seconda della specifica del caso
5.3b) Procedure operative per la gestione dei casi
5.3c) Protocolli siglati con enti, forze dell'ordine e servizi del territorio per la prevenzione e la gestione condivisa dei casi

1. INTRODUZIONE

1.1 Premessa

Una delle finalità educative del nostro Istituto è quella di favorire la formazione armonica della personalità degli alunni per rendere possibile un'adeguata integrazione sociale. Tale integrazione avviene in larga misura anche attraverso strumenti digitali che permettono la connessione ad Internet e ai social network.

I nostri bambini/ragazzi sono dunque "nativi digitali" : essi socializzano, interagiscono, comunicano, giocano, studiano attraverso tecnologie multimediali che, se usate in modo non responsabile, li espongono a rischi di cui loro stessi non sono consapevoli.

Con una diffusione apparentemente sconfinata delle tecnologie dell'informazione nella vita quotidiana, è necessario che la scuola, in quanto ente formativo, non promuova solo l'alfabetizzazione digitale, ma educhi ad una cittadinanza digitale consapevole e responsabile**.**

1.2 Scopo della Policy

La Policy di E-Safety è un documento, autoprodotto dalla scuola, attraverso il quale si esplicitano i parametri di sicurezza digitale, le norme comportamentali e le procedure per l'utilizzo delle TIC/TD in ambiente scolastico, nonché le misure per la prevenzione, per la rilevazione e la gestione delle problematiche connesse ad un uso non corretto di tali tecnologie.

La Policy tiene conto anche delle disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo previste dalla Legge n. 71 del 29 maggio 2017.

1.3 Ruoli e Responsabilità

1.3a) Ruolo della scuola nel contrasto al cyberbullismo

Ogni Istituto deve:

- individuare un referente per le iniziative contro il bullismo e il cyberbullismo;
- seguire le linee di orientamento di prevenzione e contrasto predisposte dal MIUR;
- organizzare attività di informazione-formazione rivolte ad alunni e personale scolastico;
- promuovere un ruolo attivo degli studenti;
- vigilare al fine di intercettare situazioni potenzialmente a rischio;

- intervenire in maniera repentina ed efficace qualora si verifichino atti di bullismo o cyberbullismo comprovati (da documentazione digitale o testimonianza circostanziata), anche in ambiente e in orario extrascolastico, informando i soggetti che esercitano la responsabilità genitoriale e adottando sia misure di assistenza alla vittima sia sanzioni e percorsi rieducativi per l'autore;

- denunciare alle autorità competenti eventuali reati commessi dai minori.

1.3b) Ruolo della Comunità scolastica nel rispetto della E-Policy

Tutta la Comunità Scolastica è tenuta al rispetto delle norme e dei protocolli contenuti nel presente documento e si impegna ad un uso responsabile delle TIC (Tecnologie Innovative di Comunicazione), al fine di salvaguardare la sicurezza e i diritti di tutti i Cittadini digitali (ovvero tutti coloro che si connettono ad Internet attraverso dispositivi multimediali, in ambiente scolastico ed extrascolastico).

Il personale scolastico è tenuto a vigilare, nei limiti delle proprie competenze e possibilità, affinché il presente regolamento sia rispettato e a segnalare le infrazioni secondo le procedure illustrate nel presente documento. Studenti e genitori possono segnalare al personale scolastico eventuali infrazioni di cui siano venuti a conoscenza o situazioni di disagio che li vedano direttamente coinvolti in qualità di vittime. In particolare:

DS (Dirigente scolastico):

- garantisce la corretta applicazione della E-Policy e delle linee guida in materia di bullismo e cyberbullismo, nel rispetto dei diritti, della dignità e della privacy di ciascun componente dell'istituzione scolastica;

- in collaborazione con il team per l'innovazione digitale, il responsabile per il cyberbullismo, il Collegio dei docenti ed il Consiglio d'Istituto, provvede periodicamente alla revisione della E-Policy ed alla sua integrazione con il Regolamento d'Istituto;

TID (Team Innovazione Digitale):

- vigila sulla corretta applicazione della E-Policy ;

- provvede periodicamente al suo aggiornamento anche in funzione dell'evoluzione delle tecnologie digitali;

RESPONSABILE PER IL CYBERBULLISMO:

- vigila sulla corretta applicazione della E-Policy e delle linee guida in materia di bullismo e cyberbullismo;

- provvede al suo aggiornamento periodico anche in funzione dell'evoluzione delle tecnologie digitali;
- organizza attività di informazione-formazione rivolte ad alunni, studenti e personale scolastico, in materia di bullismo, cyberbullismo e cittadinanza digitale;
- organizza percorsi rieducativi per gli alunni che non hanno rispettato le norme previste dal presente documento;
- interviene in sostegno delle vittime di bullismo o cyberbullismo.

DOCENTI:

- promuovono la cultura dell'uso consapevole e corretto delle nuove tecnologie e della rete, del rispetto della dignità e della privacy di ciascuno;
- prevengono, intercettano e segnalano situazioni legate ad un uso scorretto delle nuove tecnologie e ai rischi della rete;
- vigilano, nei limiti delle proprie competenze e possibilità, sull'uso scolastico delle nuove tecnologie e della rete;
- segnalano al dirigente e al responsabile per il cyberbullismo eventuali infrazioni al presente regolamento;
- suggeriscono al TID modifiche ed integrazioni alla stessa;
- applicano e si impegnano al pieno rispetto della E-Policy.

GENITORI:

si impegnano a :

- collaborare con la scuola nella promozione della cultura dell'uso consapevole e corretto delle nuove tecnologie e della rete, del rispetto della dignità e della privacy di ciascuno;
- prevengono e intercettano situazioni legate ad un uso scorretto delle nuove tecnologie e le segnalano alla scuola;
- vigilano, nei limiti delle proprie competenze e possibilità, sui device dei propri figli al fine di prevenire ed intercettare situazioni di rischio;

- segnalano alla scuola casi di uso scorretto delle nuove tecnologie da parte di alunni singoli o in gruppo;
- segnalano alla scuola casi di bullismo o cyberbullismo di cui vengano a conoscenza sia nei confronti dei propri figli e in un ruolo più esteso di responsabilità sociale ;
- suggeriscono alla scuola modifiche ed integrazioni alla E-Policy attraverso la figura del referente bullismo.

ALUNNI:

si impegnano a:

- rispettare la E-Policy;
- segnalare tempestivamente casi di uso scorretto delle nuove tecnologie da parte di compagni singoli o in gruppo;
- segnalare alla scuola casi di bullismo o cyberbullismo, di cui sono vittime o spettatori;
- collaborare con la scuola nella diffusione dell'uso corretto delle tecnologie digitali;
- suggerire alla scuola modifiche ed integrazioni alla E-Policy attraverso lavori suggeriti dai docenti.

RAPPRESENTANTI DI CLASSE:

- collaborano con i team docenti/Consigli di classe e la scuola alla promozione, tra i genitori, della cultura dell'uso consapevole e corretto delle nuove tecnologie e della rete, del rispetto della dignità e della privacy di ciascuno;
- raccolgono tra i genitori segnalazioni di casi di uso scorretto delle nuove tecnologie da parte di alunni singoli o in gruppo;
- segnalano alla scuola eventuali casi di bullismo o cyberbullismo di cui sono venuti conoscenza.

DSGA (Direttore dei Servizi Generali ed Amministrativi):

- vigila sulla corretta applicazione della E-Policy da parte del personale ATA;

- suggerisce al TID modifiche ed integrazioni alla stessa.

PERSONALE ATA (Amministrativo Tecnico Ausiliario):

si impegna a:

- segnalare al dirigente e al responsabile per il cyberbullismo eventuali infrazioni al presente regolamento;
- al pieno rispetto della E-Policy.

ORGANO DI GARANZIA INTERNO:

- in caso di sanzioni disciplinari, garantisce la corretta applicazione della E-Policy e del Regolamento d'Istituto, nella salvaguardia dei diritti degli alunni;
- decide, su richiesta di chiunque vi abbia interesse, anche sui conflitti che sorgano all'interno della scuola in merito all'applicazione della E-Policy e del Regolamento d'Istituto.

1.4 Condivisione e comunicazione della Policy all'intera comunità scolastica

Il presente documento, prodotto e revisionato dal TID, è condiviso con il Collegio dei Docenti e con il Consiglio d'Istituto che possono apportare eventuali modifiche ed integrazioni. Dopo l'approvazione degli Organi Collegiali preposti, il documento deve essere pubblicato sul sito scolastico affinché l'intera Comunità Scolastica possa visionarlo.

1.5 Gestione delle infrazioni alla Policy

Le infrazioni al regolamento potranno portare all'irrogazione di sanzioni disciplinari. Per tutte le infrazioni sono previsti appositi interventi educativi che:

- sono improntati ai criteri della congruità e della proporzionalità;
- sono sempre temporanei e commisurati alla gravità dell'infrazione, all'entità del danno provocato e alla recidività;
- tendono a far riconoscere ai responsabili la violazione delle norme causate dai loro gesti, ad impedirne la ripetizione, a favorire la correzione di atteggiamenti scorretti;
- sono ispirati al principio della riparazione del danno;
- tengono conto della situazione personale dell'alunno.

Per infrazioni riferibili a "mancanze disciplinari gravissime" si prevede l'attivazione del procedimento disciplinare. La gravità di una mancanza va valutata anche in base alle specificità della situazione, ad eventuali circostanze aggravanti e/o attenuanti e alla gravità del danno subito dalla vittima e/o dalla scuola.

All'alunno è sempre offerta la possibilità di impegnarsi in attività in favore dell'Istituto. I provvedimenti saranno presi con tempestività al fine di non sminuirne il valore educativo. Per i doveri generali da rispettare, le mancanze disciplinari, le sanzioni, gli interventi educativi riparatori e gli organi competenti a irrogare le sanzioni si fa riferimento alla tabella regolamento di Istituto e nello specifico:

- Art. 1 Provvedimenti disciplinari scuola primaria (D.P.R. 249 24/06/98 e D.P.R. n. 235 del 21/11/2007)
- Art. 2 Provvedimenti disciplinari scuola secondaria di I grado (D.P.R. 249 24/06/98 e D.P.R. n. 235 del 21/11/2007) allegati 2a e 2b

1.6 Procedure operative per la gestione delle infrazioni alla Policy

1.6a) Che cosa segnalare

Il personale scolastico è tenuto a segnalare:

- Situazioni potenzialmente a rischio di cyberbullismo, in particolare:
  - Alunni sorpresi a minacciare verbalmente, insultare o provocare ripetutamente compagni (in quanto il cyberbullismo generalmente si manifesta prima nella vita reale, per poi degenerare in quella virtuale)
  - Alunni che mostrano evidente disagio emotivo ed emarginati dal gruppo (in quanto possibili vittime di bullismo reale o virtuale)
- Qualunque infrazione al regolamento

Gli alunni e i genitori possono segnalare:

- Casi di cyberbullismo, cyberstalking, molestie e adescamento online, happy slapping, sexting, violazione della Privacy, accesso a contenuti non adeguati, dipendenza da Internet e qualunque altra situazione di rischio effettivo, anche se accadute in ambito extrascolastico.

1.6b) Come segnalare e a chi.

Gli alunni possono effettuare personalmente le loro segnalazioni a qualunque docente dell'Istituto o allo sportello d'ascolto presso la scuola secondaria.

I genitori possono effettuare le loro segnalazioni personalmente ai docenti di classe, al referente per il cyberbullismo, al vicepreside, al Dirigente Scolastico o allo sportello di ascolto presso la scuola secondaria.

I docenti sono tenuti ad effettuare le segnalazioni delle infrazioni ritenute gravi o gravissime al Dirigente scolastico; in caso di atti di bullismo, cyberbullismo e violazione dei diritti di cittadinanza digitale, i docenti dovranno effettuare la segnalazione anche al responsabile per il cyberbullismo.

Il responsabile dello sportello ascolto, contemperando il rispetto della privacy, la deontologia professionale e la salvaguardia del minore, dovrà segnalare quanto appreso al Dirigente Scolastico.

Il Dirigente scolastico, monitorata la situazione, potrà richiedere una relazione scritta su quanto accaduto, convocare il responsabile per il cyberbullismo, i team, o i Consigli di classe coinvolti ed eventualmente allertare gli operatori di polizia laddove sia necessario.

1.6c) Come gestire le segnalazioni.

Tenendo conto che alcune infrazioni possono configurarsi come veri e propri reati perseguibili dal codice penale, in caso di segnalazione da parte di un alunno o di un genitore, i docenti sono tenuti a:

Infrazioni ritenute lievi:

1. Verificare, nei limiti del possibile, che quanto segnalato sia realmente accaduto.
2. Approfondire con discrezione l'accaduto attraverso uno o più colloqui con i soggetti coinvolti.
3. Provvedere ad irrogare le note disciplinari .

Infrazioni ritenute gravi o gravissime o in caso di indecisione sulla gravità dell'accaduto, prima di procedere con quanto previsto al punto 2, il docente informa il Dirigente Scolastico e, se necessario, il responsabile per il Cyberbullismo, per una gestione condivisa del problema.

Si ricorda che l'infrazione della presente E-Policy da parte del personale (docente, ATA) può costituire elemento di contestazione d'addebito disciplinare e per gli esterni (esperti, collaboratori, etc.) può essere causa di risoluzione di eventuali contratti e/o convenzioni in essere.

1.7 Monitoraggio dell'implementazione della Policy e suo aggiornamento

Il TID, sulla base delle segnalazioni effettuate, rileva annualmente le esigenze dell'Istituto verificando che il documento sia una risorsa efficace, operando eventuali integrazioni o modifiche.

1.8 Integrazione della Policy con Regolamenti esistenti

Il TID, in collaborazione con la funzione strumentale PTOF (Piano Triennale dell'Offerta Formativa) e sua Commissione, con la funzione strumentale Inclusione e benessere e sua Commissione, con la funzione strumentale Comunicazione e sua Commissione, in raccordo con il Collegio Docenti, opera al fine di integrare i regolamenti dell'Istituto con il presente documento, apportandone le opportune modifiche da proporre al Consiglio d'Istituto.

2. FORMAZIONE E CURRICOLO

2.1 Curricolo sulle competenze digitali per gli studenti

La scuola deve promuovere lo sviluppo delle competenze digitali affinché gli alunni acquisiscano le conoscenze, le abilità e le attitudini necessarie per utilizzare Internet e le tecnologie digitali con dimestichezza, creatività, consapevolezza, responsabilità e spirito critico.

COMPETENZE DIGITALI IN USCITA DALLA SCUOLA PRIMARIA E SECONDARIA DI PRIMO GRADO

- Utilizzare e gestire strumenti tecnologici con dimestichezza (computer, tablet, stampanti, scanner, macchine fotografiche, ecc...).
- Utilizzare software anche open source per produrre, modificare, salvare e presentare documenti, immagini, video.
- Utilizzare Internet per studiare, reperire, scambiare e condividere informazioni e documenti, comprendendo le problematiche legate alla validità e all'affidabilità delle informazioni, usandole quindi in modo critico, accertandone la pertinenza e distinguendo il reale dal virtuale .
- Conoscere il ruolo e le opportunità delle tecnologie nella vita quotidiana privata, sociale e del mondo del lavoro.
- Essere consapevole dei potenziali rischi di Internet e della comunicazione tramite i supporti elettronici (chat, social network, email) e attuare comportamenti di prudenza e protezione adeguati a riguardo.
- Essere consapevoli delle norme e delle Leggi che regolano il corretto utilizzo di chat, social network e siti web, attuando comportamenti sociali corretti, nel rispetto del prossimo e della Legge n°71 in materia di cyberbullismo.

Ciascuna classe sviluppa le suddette competenze tenendo conto non solo dell'età degli alunni, ma anche dei prerequisiti che gli alunni già possiedono e di eventuali esigenze specifiche della classe (rilevazione di situazioni a rischio, comportamenti scorretti, ecc…).

SCUOLA PRIMARIA

Classe prima

- ✓ Riconoscere strumenti tecnologici e digitali di uso comune e comprenderne la funzione.
- ✓ Accendere e spegnere dispositivi digitali.
- ✓ Utilizzare il mouse.
- ✓ Eseguire semplici giochi ed esercizi di tipo logico, linguistico, matematico, topologico attraverso dispositivi digitali.
- ✓ Sviluppare il pensiero computazionale attraverso semplici esercizi di coding.
- ✓ Eseguire semplici algoritmi lineari attraverso attività pratiche, schede grafiche o dispositivi digitali.

Classe seconda

- ✓ Utilizzare con dimestichezza mouse e tastiera.
- ✓ Conoscere la struttura e la funzione di un computer e delle sue periferiche.
- ✓ Avviare ed eseguire semplici giochi ed esercizi di tipo logico, linguistico, matematico, topologico attraverso dispositivi digitali.
- ✓ Sviluppare il pensiero computazionale attraverso semplici esercizi di coding.
- ✓ Eseguire algoritmi attraverso attività pratiche, schede grafiche o dispositivi digitali.
- ✓ Conoscere e applicare le regole basilari di prevenzione dei rischi per la salute durante l'uso dei dispositivi digitali (postura, illuminazione, ecc...).

Classe terza

- ✓ Avviare ed eseguire in autonomia giochi ed esercizi di tipo logico, linguistico, matematico, topologico, attraverso dispositivi digitali.
- ✓ Utilizzare le procedure informatiche per la gestione del desktop e dei file.

- ✓ Utilizzare semplici software per scrivere e disegnare.
- ✓ Leggere e creare diagrammi di flusso.
- ✓ Sviluppare il pensiero computazionale attraverso esercizi di coding.
- ✓ Utilizzare mappe e schemi per studiare, progettare, programmare.
- ✓ Conoscere le potenzialità d'uso dei dispositivi digitali e di strumentazioni tecnologiche nella vita quotidiana e in ambito scientifico.

Classe quarta

- ✓ Conoscere le funzioni avanzate per la personalizzazione dei documenti (formattazione del testo, inserimento di immagini, impaginazione, ecc…).
- ✓ Creare semplici diagrammi, mappe e schemi per studiare, programmare e progettare oggetti anche digitali.
- ✓ Comprendere il funzionamento di Internet e le sue potenzialità (servizi online).
- ✓ Sviluppare il pensiero computazionale attraverso esercizi di coding.
- ✓ Utilizzare un browser per accedere a pagine prestabilite (sito della scuola, registro online, siti didattici).
- ✓ Utilizzare Internet per accedere ai materiali digitali inviati dalle insegnati tramite registro elettronico o altra piattaforma online per la condivisione dei documenti.
- ✓ Conoscere i potenziali rischi nell'uso di Internet e dei dispositive digitali (con particolare riguardo alle problematiche relative ai virus, alla validità delle fonti su Internet, alla presenza di contenuti non adeguati, alla simbologia di sicurezza sulle confezioni dei giochi, alla prevenzione delle dipendenze).
- ✓ Conoscere le norme basilari della cittadinanza digitale.

Classe quinta

- ✓ Utilizzare funzioni avanzate per la personalizzazione dei documenti (formattazione del testo, inserimento di immagini, impaginazione, ecc…).
- ✓ Creare semplici diagrammi, mappe e schemi per studiare, programmare e progettare oggetti anche digitali.
- ✓ Utilizzare software o materiale strutturato per la progettazione o la programmazione di semplici oggetti meccanici o digitali.

- ✓ Sviluppare il pensiero computazionale attraverso esercizi di coding.
- ✓ Conoscere le potenzialità di Internet come fonte di informazione.
- ✓ Utilizzare motori di ricerca per accedere a fonti di informazione necessarie per lo studio e le ricerche scolastiche.
- ✓ Utilizzare Internet per accedere ai materiali digitali inviati dalle insegnati tramite registro elettronico o altra piattaforma online per la condivisione dei documenti.
- ✓ Conoscere i potenziali rischi nell'uso di Internet e dei dispositivi digitali (con particolare riguardo alle problematiche relative alla validità delle fonti su Internet, alla presenza di contenuti non adeguati, alla simbologia di sicurezza sulle confezioni dei giochi, alla prevenzione delle dipendenze) e attuare comportamenti corretti a riguardo.
- ✓ Conoscere le norme basilari della cittadinanza digitale e attuare comportamenti corretti a riguardo.

SCUOLA SECONDARIA DI PRIMO GRADO

Classe Prima

- ✓ Sviluppare il pensiero computazionale attraverso esercizi di coding.
- ✓ Utilizzare software per creare e personalizzare documenti di vario tipo (testo, immagini, video) e fogli di calcolo.
- ✓ Creare semplici diagrammi, mappe e schemi per studiare.
- ✓ Utilizzare traduttori e vocabolari online.
- ✓ Utilizzare Internet come mezzo di informazione per reperire notizie, immagini, documenti materiali didattici.
- ✓ Utilizzare Internet per accedere ai materiali digitali inviati dalle insegnanti tramite registro elettronico o altra piattaforma online per la condivisione dei documenti.
- ✓ Conoscere le potenzialità dei dispositivi digitali come mezzi di comunicazione e socializzazione.
- ✓ Conoscere i potenziali rischi nell'uso di Internet e dei dispositivi digitali e attuare comportamenti corretti a riguardo.
- ✓ Conoscere le norme basilari della cittadinanza digitale (con particolare riguardo alle problematiche relative al cyberbullismo, al rispetto della Privacy, della Netiquette e della Legge) e attuare comportamenti corretti a riguardo.

Classe Seconda

- ✓ Sviluppare il pensiero computazionale attraverso esercizi di coding.
- ✓ Utilizzare software per creare e personalizzare documenti di vario tipo (testo, immagini, video) , presentazioni.
- ✓ Creare semplici diagrammi, mappe e schemi per studiare.
- ✓ Utilizzare traduttori, vocabolari online e altri servizi per la didattica.
- ✓ Utilizzare Internet come mezzo di informazione per reperire notizie, immagini, documenti materiali didattici.
- ✓ Utilizzare Internet per accedere ai materiali digitali inviati dalle insegnanti tramite registro elettronico o altra piattaforma online per la condivisione dei documenti.
- ✓ Utilizzare il browser nelle sue diverse funzionalità (copiare, stampare e scaricare contenuti, memorizzare siti preferiti, ecc…).
- ✓ Conoscere i potenziali rischi nell'uso di Internet e dei dispositive digitali (con particolare riguardo alle problematiche relative alle dipendenze, all'adescamento online, alla web reputation) e attuare comportamenti corretti a riguardo.
- ✓ Conoscere le norme basilari della cittadinanza digitale (con particolare riguardo alle problematiche relative al cyberbullismo, al rispetto della Privacy, della Netiquette e della Legge) e attuare comportamenti corretti a riguardo.

Classe Terza

- ✓ Sviluppare il pensiero computazionale attraverso esercizi di coding.
- ✓ Utilizzare software per creare e personalizzare documenti di vario tipo (testo, immagini, video) , fogli di calcolo, presentazioni e ipertesti.
- ✓ Creare semplici diagrammi, mappe e schemi per studiare.
- ✓ Utilizzare traduttori, vocabolari online e altri servizi per la didattica.
- ✓ Utilizzare Internet come mezzo di informazione per reperire notizie, immagini, documenti materiali didattici.
- ✓ Utilizzare Internet per accedere ai materiali digitali inviati dalle insegnati tramite registro elettronico o altra piattaforma online per la condivisione dei documenti.
- ✓ Utilizzare il browser nelle sue diverse funzionalità (copiare, stampare e scaricare contenuti, memorizzare siti preferiti, ecc…).

- ✓ Conoscere i potenziali rischi nell'uso di Internet e dei dispositive digitali (con particolare riguardo alle problematiche relative alle dipendenze, alla sindrome di Hikikomori, all'adescamento online, al sexting, alla web reputation, killfie) e attuare comportamenti corretti a riguardo.
- ✓ Conoscere le norme basilari della cittadinanza digitale (con particolare riguardo alle problematiche relative al cyberbullismo, al rispetto della Privacy, della Netiquette e della Legge) e attuare comportamenti corretti a riguardo.

2.2 Formazione dei docenti

Per poter promuovere l'utilizzo e l'integrazione delle TIC nella didattica e per formare gli alunni ad un uso consapevole e sicuro di Internet, si rende necessario un progetto di aggiornamento per tutti i docenti.

Dopo aver rilevato le competenze specifiche a livello informatico del personale e i bisogni formativi , l'Istituto deve attivare nel triennio percorsi di aggiornamento con i seguenti contenuti:

- ❖ Uso del computer e di Internet (livello base – livello intermedio).
- ❖ Uso di software per la didattica (livello base – livello medio).
- ❖ Uso della LIM e didattica digitale.
- ❖ Uso dei laboratori.
- ❖ Condivisione e comunicazione in rete.
- ❖ Impatto delle TIC sugli apprendimenti negli studenti con Bisogni Educativi Speciali.
- ❖ Rischi in Internet e uso responsabile delle TIC nel rispetto dei diritti della Cittadinanza Digitale.
- ❖ Coding.

Tali corsi potranno essere riproposti nel triennio successivo, se necessario, per aggiornare il personale scolastico di nuova immissione in ruolo o trasferito. Ci si potrà avvalere delle risorse interne all'Istituto o rivolgersi a Enti preposti.

2.3 Sensibilizzazione delle famiglie

La tutela dei minori dai pericoli della rete è un atto di responsabilità collettiva che deve essere condivisa da genitori, istituzioni e forze dell'ordine. Per raggiungere questo obiettivo è necessario non solo formare gli alunni ad un uso responsabile della rete, ma anche sensibilizzare le famiglie e fornirgli tutte le indicazioni necessarie per conoscere i mezzi a loro disposizione per

proteggere i figli quando sono online. L'Istituto Comprensivo metterà pertanto in atto una campagna di sensibilizzazione delle famiglie, suddivisa in più fasi:

- Pubblicazione sul sito del progetto Generazioni Connesse.
- Pubblicazione sul sito di video illustrativi a fumetti per ragazzi e famiglie.
- Pubblicizzazione di helpline a cui alunni, docenti e genitori si possono rivolgere.
- Distribuzione di una brochure illustrativa sui pericoli della rete.
- Organizzazione di uno o più incontri informativi per i genitori.

3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA

3.1 Protezione delle strumentazioni e della navigazione

La scuola dovrà dotarsi entro il triennio di tutte le strumentazioni tecniche necessarie per :

Proteggere la privacy del personale scolastico, degli alunni e delle loro famiglie, soprattutto per quel che riguarda i dati sensibili.

Garantire la navigazione sicura nei computer dell'Istituto.

Rivolgendosi a personale tecnico qualificato, la scuola dovrà dotarsi di:

Antivirus (software per il monitoraggio e la rimozione di virus, spyware, hardware).

Browser protetti (controllo parentale e classificazione di contenuti, eventualmente anche browser specifici per bambini).

Filtri (sistemi in grado di bloccare in modo automatico l'utilizzo di determinati servizi o l'accesso a siti e contenuti potenzialmente dannosi per bambini e adolescenti. Alcuni software bloccano le informazioni in entrata, come le email o impediscono che i bambini forniscano informazioni riservate come il proprio nome, l'indirizzo o il numero di telefono).

Utenti diversificati (Utente docente protetto da password e utente alunni con restrizioni).

3.2 Gestione accessi

3.2a) Accesso alle strumentazioni scolastiche

Il personale scolastico è tenuto a seguire le seguenti regole di accesso alle strumentazioni:

È consentito l'uso delle strumentazioni scolastiche esclusivamente per uso didattico.

Usi diversi da questo vanno autorizzati dal Dirigente Scolastico.

Le strumentazioni scolastiche devono essere maneggiate con attenzione al fine di evitarne danni strutturali. Le strumentazioni, dopo essere state utilizzate, vanno riposte con cura e non separate dagli accessori d'uso (caricabatterie, mouse…).

Il personale scolastico è tenuto a segnalare tempestivamente al responsabile della custodia delle strumentazioni la mancanza delle stesse o di eventuali accessori. Le strumentazioni vanno custodite in appositi armadi provvisti di serratura.

Il personale docente non è tenuto a creare nuovi utenti sulle strumentazioni scolastiche. L'utente riservato ai docenti deve essere provvisto di password (che non deve essere comunicata in nessun casi agli alunni). Non è consentito il salvataggio di documenti personali (bollette telefoniche, cedolini stipendi, ecc). È vietato installare software ad uso non didattico.

Gli alunni sono tenuti a rispettare le seguenti regole d'accesso alle strumentazioni:

È consentito l'uso delle strumentazioni scolastiche esclusivamente per uso didattico, secondo le disposizioni del docente presente. Le strumentazioni, dopo essere state utilizzate, vanno riposte con cura e non separate dagli accessori d'uso (caricabatterie, mouse…).

Le strumentazioni scolastiche devono essere maneggiate con attenzione al fine di evitarne danni strutturali. Gli alunni possono accedere solo all'utente a loro riservato, libero da password. È consentito il salvataggio di documenti personali a scopo didattico, utilizzando cartelle specifiche per ciascuna classe.

3.2b) Accesso alla rete scolastica

In ogni plesso è presente un modem-router che permette la messa in rete e la connessione ad Internet dei dispositivi presenti nell'edificio. Per accedere alla rete è necessario che il dispositivo sia collegato tramite cavo o con WiFi. Per connettere un dispositivo al WiFi scolastico è necessario inserire la chiave di sicurezza, custodita dall'Amministratore delle reti**.**

3.2c) Accesso ad Internet

Il personale scolastico è tenuto a seguire le seguenti regole di accesso ad Internet:

- ☞ È possibile accedere ad Internet attraverso strumentazioni in dotazione all'istituto o attraverso dispositivi personali.

- ☞ L'accesso ad Internet e la navigazione attraverso le strumentazioni scolastiche è riservato ad un uso strettamente didattico.
- ☞ È possibile accedere ad account personali durante l'uso di Internet, ma è obbligatorio il logout al termine.
- ☞ Non è consentito il salvataggio di dati personali (nomi utenti, account e password) nei browser delle strumentazioni scolastiche.
- ☞ È vietato scaricare o installare da Internet materiale potenzialmente dannoso, di provenienza non sicura o non legale.

Gli alunni sono tenuti a rispettare le seguenti regole d'accesso ad Internet:

- ☞ È vietato l'accesso ad Internet senza autorizzazione da parte del personale docente.
- ☞ È vietata la navigazione in assenza del docente.
- ☞ L'accesso ad Internet e la navigazione attraverso le strumentazioni scolastiche è riservato ad un uso strettamente didattico e nel rispetto di diritti della cittadinanza digitale e delle norme vigenti di utilizzo legale della rete.
- ☞ È vietato il salvataggio di dati personali (nomi utenti, account e password) nei browser delle strumentazioni scolastiche.
- ☞ È vietato scaricare da Internet materiale senza l'autorizzazione del docente.

Tutti gli operatori presenti a qualsiasi titolo nella scuola (esperti esterni, collaboratori, ditte esterne...) e i genitori che accedono all'edificio scolastico, dovranno attenersi alle regole generali previste per il personale.

3.3 Email

Tutte le comunicazioni scolastiche dovranno progressivamente avvenire attraverso canali digitali. Il personale scolastico deve essere in possesso di un indirizzo di posta istituzionale (istruzione.it) e comunicarlo in segreteria all'atto dell'assunzione presso l'istituto: le comunicazioni ufficiali e l'invio di documenti in segreteria deve avvenire esclusivamente attraverso la posta istituzionale o altra posta certificata e non attraverso altri indirizzi privati non verificabili. Il personale scolastico, le famiglie, gli operatori esterni e gli Enti potranno comunicare con la segreteria inviando la posta all'indirizzo a disposizione dell'Istituto:

coic84200n@istruzione.it

coic84200n@pec.istruzione.it

3.4 Sito web della scuola

Il sito scolastico è stato ristrutturato e ha i seguenti parametri: htt://www.iccucciago.edu.it

Il sito scolastico deve essere aggiornato secondo le norme vigenti sulla trasparenza e in particolare:

- La pubblicazione delle informazioni e delle circolari nella Homepage, nell'Albo online e nell'Amministrazione Trasparente è a cura del personale di segreteria.
- Le altre sezioni e la struttura stessa del sito vengono aggiornate annualmente o secondo necessità.
- L'accesso alla sezione amministrativa del sito scolastico è riservata al Dirigente Scolastico e/o al suo delegato, al personale di segreteria.
- L'accesso alla parte pubblica del sito è libera.

3.5 Social network

È vietato al personale scolastico e agli alunni di accedere a social network e chat attraverso le strumentazioni della scuola, se non per uso didattico. In caso di progetti che ne prevedano l'uso, il docente è tenuto a comunicarlo preventivamente al Dirigente Scolastico e a monitorare gli alunni affinché ne facciano un uso corretto, secondo le disposizioni dell'insegnante.

È comunque vietato pubblicare sui social network o su qualunque sito Internet documenti, foto, registrazioni audio-video che possano essere lesivi per la reputazione o per la privacy degli alunni e del personale scolastico. Segnalazioni di infrazioni possono essere comunicate secondo il protocollo presente al capitolo 5.

3.6 Registro scolastico

Il registro elettronico online è uno strumento al quale possono accedere tutti i membri della Comunità Scolastica, previa registrazione da parte della segreteria. Tutti gli utenti devono essere provvisti di nome utente e password. L'uso del registro è personale e riservato: ogni utente deve provvedere affinché i dati di login restino riservati e si impegna a cambiare password nel caso in cui la riservatezza degli stessi sia stata violata.

3.6a) Area Amministrativa

Il Dirigente scolastico, il personale di segreteria e l'Amministratore del registro possono accedere a specifiche aree riservate, personalizzate secondo ruoli e mansioni stabilite, per configurare le impostazioni di sistema e inviare comunicazioni al personale. Tutte le comunicazioni ufficiali devono passare attraverso l'apposita area del registro.

3.6b) Area Docenti

Il personale scolastico può accedere solo all'area riservata ai docenti. I dati di accesso all'account devono essere richiesti personalmente in segreteria. Le richieste di assegnazione di ambito e altre eventuali configurazioni vanno richieste previa segnalazione al Ds e all'Amministratore del registro.

Il personale scolastico:

- ☞ È tenuto a leggere le comunicazioni ufficiali della segreteria.
- ☞ Può inviare comunicazioni e avvisi ai genitori tramite l'apposita sezione. Può pubblicare e condividere con docenti e alunni materiale didattico.
- ☞ Deve registrare quotidianamente le presenze e firmare il registro di classe .
- ☞ Deve tenere periodicamente aggiornate le sezioni riguardanti la programmazione, i voti e l'agenda di classe. Deve compilare le proposte di voto e i documenti di valutazione entro i termini previsti per lo scrutinio.
- ☞ Deve comunicare alla segreteria eventuali incongruenze nell'elenco degli alunni
- ☞ Deve segnalare all'Amministratore del registro eventuali anomalie nel funzionamento.

3.6c) Area esercenti responsabilità genitoriali

I genitori accedono all'apposita sezione ad essi riservata ai tutori ed hanno a disposizione un account I dati di accesso all'account vengono consegnati ai genitori dalla segreteria.

I genitori:

- ☞ Sono tenuti a leggere le comunicazioni ufficiali della segreteria e dei docenti.
- ☞ Devono controllare quotidianamente il registro, in particolare le assenze, i voti, le note, i documenti di valutazione e l'agenda di classe.

- Devono comunicare alla segreteria eventuali incongruenze nei dati anagrafici personali o del proprio figlio.
- Devono segnalare ai docenti eventuali anomalie nel funzionamento o incongruenze nei dati inseriti.
- Devono mantenere riservati i dati di accesso.

3.7 Protezione dei dati personali

Si ricorda a tutto il personale scolastico che il segreto professionale o d'ufficio obbliga a non rivelare le informazioni aventi natura di segreto, secondo un codice etico (legato al rispetto della persona), deontologico (come norma di comportamento professionale) e giuridico.

È conseguentemente vietato al personale scolastico di divulgare personalmente o di pubblicare su blog, social network o siti personali qualunque informazione possa violare il segreto d'ufficio.

3.7a) Procedure operative per la protezione dei dati personali.

Per quanto riguarda dati di accesso a strumentazioni, reti WiFi o registri, **tutti i dipendenti** devono custodire i dati di accesso facendo attenzione che terzi non ne vengano a conoscenza. Nel caso in cui sia violata la segretezza di una password, l'Amministratore del registro deve provvedere alla sua immediata sostituzione.

Il **personale scolastico**, nello svolgimento delle proprie mansioni, deve prestare particolare attenzione a:

- Non divulgare ad estranei le informazioni di cui viene a conoscenza durante il servizio.
- Non fare copie, per uso personale, dei dati sensibili.
- Osservare i criteri di riservatezza.
- Trattare i dati in modo lecito e secondo correttezza.
- Trattare i dati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati.
- Comportarsi nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di

distruzione, di perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Il personale di segreteria è inoltre tenuto a:

Adottare delle cautele nella trasmissione, nella riproduzione e nella distruzione dei documenti contenenti dati personali, al fine di prevenire eventuali rischi di accesso ai dati da parte di soggetti non autorizzati. Per tutte le procedure inerenti la sicurezza e la gestione dei dati fare riferimento ai documenti interni previsti dalle norme.

L'Amministratore di rete, il Webmaster, l'Amministratore del sito, l' Amministratore del registro e l'Assistente tecnico, che possiedono dati di accesso a reti, siti, registri, strumentazioni per lo svolgimento delle specifiche mansioni, sono inoltre tenuti a:

- Non comunicare a persone non autorizzate i dati di accesso di terzi in loro possesso
- Non utilizzare i dati di accesso di terzi senza motivata ragione.

L'Amministratore di rete, appositamente nominato dal DS, dovrà provvedere al salvataggio di backup periodici su supporti esterni che dovranno essere opportunamente conservati e non accessibili a persone non autorizzate.

4. STRUMENTAZIONE PERSONALE

4.1 Studenti

Non è consentito l'uso di dispositivi personali (notebook, tablet, cellulare, ecc …), se non previamente autorizzata dai docenti, in modo temporaneo e per esclusive attività didattiche fatta eccezione per gli alunni con DSA o diversamente abili per i quali ci sia evidenza di averne necessità per un uso strettamente didattico o per la comunicazione: in questo caso i genitori dovranno farne richiesta scritta documentata al Dirigente.

I team o i Consigli di classe successivamente provvederanno ad approvare o a respingere la richiesta con propria decisione motivata. Viceversa, i team o i consigli di classe potranno promuovere, per gli alunni per i quali ci sia evidenza che l'uso di dispositivi personali possa migliorare il percorso didattico e rimuovere ostacoli all'apprendimento, con la condivisione delle famiglie, l'uso di device personali. L'uso di dispositivi personali (notebook, tablet, cellulare, ecc …), finalizzato a singole attività, può comunque essere autorizzato dai docenti e sotto la loro

responsabilità. L'Istituto non sarà comunque ritenuto responsabile in caso di furto o danneggiamento accidentale. In tal caso, l'uso delle strumentazioni personali e l'accesso ad Internet è regolato dalle norme al capitolo 3.2.

Nell'edificio scolastico e nell'area di pertinenza, è vietato registrare foto, video e audio con dispositivi digitali personali se non con l'autorizzazione dei docenti e per attività programmate. Non è comunque consentito l'uso del cellulare a scuola per l'invio e la ricezione di messaggi (SMS, MMS, ecc) e telefonate personali, né per l'accesso ad Internet e alle piattaforme Social (Facebook, Whatsapp, ecc...).

In caso di uscite didattiche, viaggi d'istruzione, recite, progetti sul territorio ed altre situazioni affini, valgono le stesse regole delle normali attività didattiche. Tuttavia, i docenti accompagnatori potranno comunicare agli alunni e ad eventuali genitori presenti, quali dispositivi digitali sono consentiti (cellulari, macchine fotografiche, videocamere, Ipad, Ipod...) e le regole di utilizzo. L'Istituto non sarà ritenuto responsabile in caso di furto o danneggiamento accidentale. Le foto e i video eventualmente registrati in queste occasioni, dietro autorizzazione dei docenti, dovranno avere un uso personale e non potranno essere diffusi in rete qualora siano state riprese terze persone (altri alunni, genitori, docenti ed operatori).

4.2 Docenti

È consentito l'uso di strumentazioni personali (notebook, tablet…) per attività didattiche o extracurricolari, ma l'Istituto non sarà ritenuto responsabile in caso di furto o danneggiamento accidentale.

L'uso di Internet per fini personali, attraverso dispositivi privati, non è consentito durante l'orario di servizio; è invece consentito al di fuori dell'orario di servizio, nel rispetto dei diritti della cittadinanza digitale e delle norme vigenti di utilizzo legale della rete. Non è, comunque, consentito l'acceso ad Internet attraverso la rete scolastica per fini personali.

Non è consentito l'uso del cellulare durante l'orario di servizio se non per attività didattiche.

In caso di viaggi d'istruzione, recite, progetti sul territorio ed altre situazioni affini, foto e video potranno essere pubblicati su giornalini scolastici o sul sito dell' Istituto se la famiglia ne ha firmato il consenso.

4.3 Personale amministrativo e i collaboratori scolastici

Per garantire la sicurezza dei dati sensibili, non è consentito svolgere attività amministrativa su dispositivi informatici personali (notebook, tablet...). Non è, comunque, consentito l'acceso ad Internet attraverso la rete scolastica per fini personali.

Non è, inoltre, consentito l'uso del cellulare per fini personali durante l'orario di servizio.

4.4 Altri operatori

Tutti gli altri operatori presenti a qualsiasi titolo nella scuola (esperti esterni, collaboratori, ditte esterne...) dovranno attenersi alle norme previste per il personale scolastico.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

5.1 Prevenzione

L'uso di dispositivi digitali non è solo un passatempo, ma offre numerose opportunità di sviluppo e di apprendimento. I genitori e gli insegnanti possono sfruttare questo potenziale in modo mirato nell'educazione quotidiana. Tuttavia, dove ci sono opportunità, si nascondono anche rischi. Evitare ogni contatto dei bambini e dei giovani con Internet non è né possibile né sensato.

La prevenzione, invece, è lo strumento più efficace per proteggere i minori dai pericoli online. Per questo è importante che i giovani imparino a valutare criticamente i contenuti, riconoscano i possibili rischi e sappiano come proteggersi.

I genitori e gli insegnanti svolgono un'importante funzione di accompagnamento in questo contesto, in qualità di interlocutori di fiducia pronti a condividere esperienze e ad intervenire attivamente se necessario.

5.1a) Rischi

Il problema della sicurezza online non è riconducibile esclusivamente all'esistenza di atti criminali, più o meno conosciuti e insidiosi, di cui i ragazzi possono cadere vittima, ma anche alla possibilità che l'utilizzo di tali strumenti tecnologici, nell'arco della giornata di un ragazzo, cominci a prevalere a scapito di spazi di aggregazione concreti, attività sociali, ricreative e sportive.

Quando i ragazzi cominciano a soddisfare, attraverso questi strumenti, bisogni profondi che dovrebbero trovare risposta nella vita reale, allora ne fanno un utilizzo sostitutivo anziché integrativo, esponendosi al rischio di isolamento o di dipendenza. Inoltre, una conoscenza limitata e parziale delle norme che regolano l'utilizzo di Internet, creano maggiori possibilità che gli stessi ragazzi le infrangano, più o meno inconsapevolmente.

I rischi più comuni in rete sono rappresentati da:

- Adescamento Online
- Cyberbullismo

- ❖ Cyberstalking
- ❖ Happy slapping
- ❖ Sexting
- ❖ Violazione della Privacy
- ❖ Accesso a contenuti non adeguati
- ❖ Dipendenza da Internet
- ❖ Gioco d'azzardo e siti di realtà virtuale

5.1b) Azioni per la riduzione dei rischi

L'Istituto si prefigge di intraprendere le seguenti azioni per la prevenzione dei rischi online:

- ☞ Monitorare la realtà dell'istituto per ridurre il grado di rischio relativo ad eventi problematici (in particolare violazione della privacy, cyberbullismo, accesso a contenuti non adeguati)
- ☞ Rafforzare la competenza mediatica dei docenti attraverso la formazione
- ☞ Per poter assumere l'importante funzione di accompagnamento gli insegnanti devono conoscere bene il mondo digitale per essere in grado di valutare in modo obiettivo i potenziali pericoli che vi si celano.
- ☞ Sensibilizzare la Comunità Scolastica al problema dei rischi legati ad un uso non responsabile di Internet e dei social network (con incontri informativi per i genitori e la pubblicizzazione attraverso brochure e video)
- ☞ Promuovere progetti per la responsabilizzazione degli alunni in qualità di Cittadini Digitali Insegnando agli alunni ad essere responsabili nell'uso dei dispositivi digitali, forniamo loro un essenziale strumento sia per proteggersi da situazioni a rischio, sia per evitare di diventare loro stessi cyberbulli.

5.2 Rilevazione

5.2a) Che cosa segnalare

Il personale scolastico è tenuto a segnalare**:**

- Situazioni potenzialmente a rischio di cyberbullismo, in particolare:
  - Alunni sorpresi a minacciare verbalmente, insultare o provocare ripetutamente compagni (in quanto il cyberbullismo generalmente si manifesta prima nella vita reale, per poi degenerare in quella virtuale)
  - Alunni che mostrano evidente disagio emotivo ed emarginati dal gruppo (in quanto possibili vittime di bullismo reale o virtuale)
- Qualunque infrazione al Regolamento
- Strumentazioni che presentano potenziali falle nella sicurezza della navigazione

Gli alunni e i genitori possono segnalare:

- Casi di cyberbullismo, cyberstalking, adescamento online, happy slapping, sexting , violazione della Privacy , accesso a contenuti non adeguati, dipendenza da Internet e qualunque altra situazione di rischio effettiva, anche se accadute in ambito extrascolastico.

5.2b) Come segnalare e a chi

Gli alunni possono effettuare personalmente le loro segnalazioni a qualunque docente dell'Istituto, anche in forma riservata, o allo sportello d'ascolto presso la scuola secondaria (le modalità di accesso allo sportello vengono delineate agli alunni all'inizio di ogni anno scolastico).

I genitori possono effettuare le loro segnalazioni personalmente ai docenti di classe, alla vicepreside, al responsabile per il cyberbullismo, al Dirigente Scolastico o allo sportello di ascolto presso la scuola secondaria. Le modalità di contatto vengono annualmente delineate all'inizio di ogni anno scolastico. Il Dirigente Scolastico potrà, comunque, essere contattato telefonicamente o tramite la email istituzionale, anche al solo scopo di fissare un appuntamento.

I docenti sono tenuti ad effettuare le segnalazioni al DS e a coinvolgere il team/consiglio di classe, l'Animatore Digitale e il responsabile per il cyberbullismo.

Il Dirigente Scolastico, monitorata la situazione, potrà richiedere una relazione scritta su quanto accaduto ed eventualmente allertare gli operatori di polizia laddove sia necessario

La collaborazione scuola-famiglia è di vitale importanza al fine di promuovere un uso consapevole dei nuovi media e quindi oltre a condividere informazioni sulla sicurezza in rete, sul suo corretto utilizzo e sui potenziali pericoli è necessario anche informare circa possibili strategie di intervento qualora si rilevassero abusi.

La linea di ascolto 1.96.96 (attiva 24 ore su 24, 365 giorni all'anno) e la chat (attiva tutti i giorni dalle 8.00 alle 22.00 (sabato e domenica dalle 8.00 alle 20.00) di **Telefono Azzurro** accolgono qualsiasi richiesta di ascolto e di aiuto da parte di bambini/e e ragazzi/e fino ai 18 anni o di adulti che intendono confrontarsi su situazioni di disagio/pericolo in cui si trova un minorenne.

Il servizio di **Helpline** è riservato, gratuito e sicuro, dedicato ai giovani o ai loro familiari che possono chattare, inviare email o parlare al telefono con professionisti qualificati relativamente a dubbi, domande o problemi legati all'uso delle nuove tecnologie digitali e alla sicurezza online.

Inoltre, è disponibile il servizio **Hotline** che si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la rete.

I due servizi messi a disposizione dal Safer Internet Center sono il "**Clicca e Segnala"** di **Telefono Azzurro** e **"STOP-IT"** di **Save the Children.** Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia.

Anche la **Polizia Postale e delle Comunicazioni** è attualmente impegnata in diverse attività a sostegno della navigazione protetta dei minori ed è competente a ricevere segnalazioni su qualsiasi tipo di reato informatico.

5.2c) Come gestire le segnalazioni.

In caso di segnalazione da parte di un alunno o di un genitore, o su sollecitazione del DS (nel caso la segnalazione sia pervenuta direttamente al DS), i docenti sono tenuti a:

- ☞ Verificare, nei limiti del possibile, che quanto segnalato sia realmente accaduto
- ☞ Approfondire l'accaduto attraverso uno o più colloqui, possibilmente riservati, con le persone coinvolte
- ☞ Seguire il protocollo per le gestione dei casi (per una gestione condivisa del problema)

5.3 Gestione dei casi

5.3a) Definizione delle azioni da intraprendere a seconda della specifica del caso

Intervenire in situazioni di cyberbullismo/sexting/adescamento online non è mai semplice. Spesso si pensa di non sapere esattamente cosa fare e si ha timore di essere inadeguati. Nei casi in cui invece si ha un'idea teorica di come si potrebbe agire, il timore può invece essere quello di non avere i tempi e gli strumenti adeguati. L'importante è non agire in solitudine e, soprattutto, non fare scelte improvvisate, magari sull'onda delle emozioni del momento, sulle azioni da intraprendere.

I docenti, pertanto, avuta notizia di un caso (dagli alunni, dai genitori o da qualsiasi altra fonte) e seguite le indicazioni del punto c) del paragrafo 5.2, prima di intraprendere qualsiasi azione, sottoporranno la questione al Dirigente Scolastico e/o al responsabile per il cyberbullismo e si confronteranno successivamente con il team/Consiglio di Classe. Successivamente, sulla scorta degli strumenti delineati al successivo punto b), che descrivono la sequenza delle possibili azioni da intraprendere, e in accordo con il Dirigente Scolastico, il responsabile per il cyberbullismo e il team/consiglio di classe, si deciderà il percorso da seguire e se ne terrà traccia.

L'obiettivo a lungo termine della comunità scolastica è quello di creare una memoria condivisa non solo di ciò che accade nella scuola rispetto al web, ma anche di strutturare una fonte esemplificativa che possa orientare sempre più e sempre meglio le azioni di contrasto ad episodi che, nel tempo, potrebbero ripetersi.

5.3b) Procedure operative per la gestione dei casi.

Sul sito dell'Istituto sono presenti alcuni allegati che delineano i percorsi da intraprendere in funzione del singolo caso. Lo scopo di questi strumenti operativi è agevolare la decisione su come intervenire e tener traccia di ciò che è avvenuto rispetto ai comportamenti degli alunni online e di come il caso è stato gestito.

5.3c) Protocolli siglati con enti, forze dell'ordine e servizi del territorio per la prevenzione e la gestione condivisa dei casi.

La scuola ha in essere specifici accordi con la Polizia postale, per percorsi formativi nella scuola secondaria di primo grado, per la prevenzione, l'intercettazione (sportello di ascolto nella scuola secondaria) e la gestione dei casi anche in accordo con i servizi sociali comunali, oltre al supporto ai docenti, ai genitori ed agli alunni.