# 1. INTRODUZIONE

## 1.1 SCOPO DELL'E-SAFETY POLICY

Il presente documento indica procedure, misure ed azioni da adottare e promuovere al fine di:

- favorire l'assunzione di competenze digitali;
- favorire l'utilizzo delle TIC anche nella didattica;
- favorire l'adozione di misure di prevenzione e di gestione di situazioni a rischio relative all'uso di Internet e delle tecnologie digitali;
- rilevare e saper affrontare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso delle TIC;
- garantire la riservatezza nell'uso dei dati personali e/o sensibili. Il documento è rivolto a:
- tutto il personale dell' l'IC "Garibaldi" di Chiavenna (dirigenti, docenti, personale amministrativo ed ausiliario);
- tutti i genitori e gli alunni che frequentano l'IC "Garibaldi" di Chiavenna;
- tutti gli operatori esterni alla scuola, ma che interagiscono con la stessa (servizi sociali, forze dell'ordine, ecc.).

## 1.2 RUOLI E RESPONSABILITÀ

### 1.2.1 Il Dirigente Scolastico (DS)

- è il responsabile della sicurezza del sistema informatico dell'Istituto e della trasmissione e ricezione dei dati on-line;
- favorisce l'organizzazione di incontri formativi per il personale;
- favorisce l'attivazione di progetti inerenti l'uso delle TIC rivolti agli alunni;
- gestisce i rapporti con tutti gli operatori esterni alla scuola (servizi sociali, forze dell'ordine, ecc.);

### 1.2.2 Il Dirigente Amministrativo (DSGA)

- è responsabile del funzionamento e mantenimento dei diversi canali di comunicazione della scuola relativamente:
  - al programma di intervento di tecnici per l'assistenza informatica
  - alla riservatezza delle credenziali, alla rete wi-fi della scuola e gestisce le chiavi di accesso al sistema informatico della scuola.

### 1.2.3 L'Animatore Digitale:

- promuove l'aggiornamento dei docenti relativamente alla conoscenza e all'uso delle TIC;
- supporta tecnicamente l'attività di laboratorio con consigli, aiuti e chiarimenti;
- monitora l'utilizzo delle TIC e segnala al DSGA eventuali problemi che richiedono aggiornamenti nella parte software/hardware o interventi tecnici di

manutenzione;

- cura la comunicazione esterna in merito all'uso delle tecnologie informatiche e le loro ricadute sulla didattica;
- fornisce al personale consulenza e informazioni in relazione ai rischi on line e alle misure di prevenzione e gestione degli stessi.

1.2.4 Il Docente con funzione strumentale per il sito:

- curailsitowebdellascuolapergliscopiistituzionaliconsentiti;

1.2.5 Il Docente referente dell'Istituto per la prevenzione al cyber bullismo

- collabora con i docenti nominati prima;
- prepara attività e promuove strategie per lo sviluppo delle competenze digitali degli studenti, finalizzate ad un utilizzo critico della rete, delle tecnologie della società dell'informazione *(TSI)* e dei media;

- raccoglie e diffonde nuove pratiche educative collaborando con tutti gli organi rappresentativi della scuola, incontrando genitori, alunni e rappresentanti del territorio.

1.2.6 I Docenti:

- illustrano agli studenti le regole di utilizzo contenute nel presente documento garantendo che gli stessi le osservino;
- danno chiare indicazioni sul corretto utilizzo della strumentazione multimediale e di internet;
- controllano l'uso delle tecnologie digitali, dei dispositivi mobili, delle macchine fotografiche, da parte degli alunni durante le lezioni e ogni altra attività scolastica programmata;
- segnalano prontamente eventuali malfunzionamenti o danneggiamenti hardware/software all'animatore digitale o al DSGA;
- segnalano al DS eventuali abusi rilevati a scuola in relazione all'utilizzo delle tecnologie digitali o di internet.

1.2.7 Il personale amministrativo ed ausiliario è tenuto a:

- conoscere le norme di sicurezza informatica dell'Istituto;
- segnalare qualsiasi abuso al DS.

1.2.8 Gli studenti:

- sono tenuti a conoscere il regolamento d'Istituto riguardo l'uso di telefoni cellulari, telecamere e mezzi informatici attraverso attività di orientamento all'uso delle TIC;
- in caso di malfunzionamenti della strumentazione e/o di contatto accidentale con informazioni, immagini e/o applicazioni inappropriate devono comunicarlo immediatamente all'insegnante;
- non devono modificare la configurazione di sistema delle macchine;
- non devono utilizzare la strumentazione della scuola a scopi personali, ludici e/o ricreativi (a meno che l'attività didattica non lo preveda esplicitamente);
- non devono utilizzare propri dispositivi esterni personali senza aver ricevuto il preventivo permesso da parte dell'insegnante;

- nell’aula di informatica devono archiviare i propri documenti in maniera ordinata e facilmente rintracciabile in una cartella personale (con il proprio nome e classe) creata all’interno della cartella documenti dell’account loro destinato;

1.2.9 I genitori:

- sono tenuti a conoscere e far rispettare ai figli il regolamento d’Istituto riguardo l’uso di telefoni cellulari, telecamere e mezzi informatici.

1.2.10 Gli attori esterni:

- sono tenuti a conoscere e rispettare il regolamento d’Istituto riguardo l’uso di telefoni cellulari, telecamere e mezzi informatici.

## 1.3. CONDIVISIONE E COMUNICAZIONE DELLA POLICY ALL’INTERNO DELLA COMUNITA’ SCOLASTICA.

Il presente documento di *e-Safety Policy* sarà oggetto di revisione periodica da parte dell’intera comunità scolastica a seguito dall’approvazione degli organi collegiali.
La condivisione e la comunicazione del documento avverrà attraverso il sito della Scuola.
Copia dello stesso sarà esposta all’albo di ogni singolo plesso.

L’animatore digitale si farà promotore di incontri di chiarimento per tutti coloro che necessitino di ulteriori informazioni.

## 1.4 GESTIONE DELLE INFRAZIONI DELLA POLICY.

Le infrazioni alla gestione della *e-Safety Policy*, sia da parte delle figure professionali che degli alunni della scuola, saranno poste all’attenzione del DS che prenderà i necessari provvedimenti come da Regolamento d’istituto.

## 1.5 MONITORAGGIO ED IMPLEMENTAZIONE DELLA E-SAFETY POLICY E SUO AGGIORNAMENTO

Il monitoraggio e l’implementazione della Policy verrà curata dal DS in collaborazione con la Funzione Strumentale, l'Animatore Digitale che promuoveranno gli eventuali aggiornamenti che si rendano opportuni, secondo una logica di condivisione con tutto il corpo docente, le famiglie e il personale.

## 1.6 INTEGRAZIONE DELLA POLICY CON DOCUMENTI ESISTENTI

Il presente documento s’integra con gli obiettivi e i contenuti dei seguenti documenti: PTOF, Regolamento d'Istituto, Patto Educativo di corresponsabilità, la Procedura 14 (Accesso e utilizzo delle postazioni multimediali)

## 2. FORMAZIONE E CURRICOLO

### 2.1 Curricolo sulle competenze digitali per gli studenti

La raccomandazione 2006/962/CE del Parlamento Europeo e del Consiglio dell'Unione Europea individua il quadro di riferimento europeo in materia di competenze chiave per l'apprendimento permanente. Tra queste è citata la competenza digitale, "*saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione*".

Al fine di promuovere l'acquisizione e l'incremento delle competenze digitali, verranno svolte attività trasversali dirette a perseguire i seguenti obiettivi:

1. conoscere e acquisire consapevolezza su natura, ruolo e opportunità delle TSI nella vita quotidiana e professionale;
2. distinguere il reale dal virtuale;
3. sviluppare le abilità di base nelle TSI (saper usare il computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni);
4. usare le informazioni in modo critico, accertandone la provenienza e l'affidabilità;
5. acquisire consapevolezza su come le TSI possono favorire la creatività e l'innovazione;
6. acquisire consapevolezza sulle opportunità e sui potenziali rischi di Internet e della comunicazione tramite i supporti elettronici;
7. riflettere sui fondamenti di base che si pongono nell'uso interattivo delle TSI (netiquette, privacy).

### 2.2 FORMAZIONE DEI DOCENTI SULL'UTILIZZO E L'INTEGRAZIONE DELLE TIC NELLA DIDATTICA.

Sulla base delle proposte formulate annualmente dall'Animatore Digitale si provvede a stilare un piano di formazione di corsi certificati che all'occorrenza sarà suscettibile di variazioni.

### 2.3 FORMAZIONE DEI DOCENTI SULL'UTILIZZO CONSAPEVOLE E SICURO DI INTERNET E DELLE TECNOLOGIE DIGITALI.

La scuola promuove e favorisce:

- la partecipazione dei docenti ad incontri di formazione sull' uso responsabile e sicuro delle nuove tecnologie;
- eventuali incontri con le forze dell'Ordine locali.

### 2.4 SENSIBILIZZAZIONE DELLE FAMIGLIE

I corsi di formazione sull'uso responsabile e sicuro delle nuove tecnologie organizzati dalla scuola prevedono il coinvolgimento attivo delle famiglie.

La scuola, inoltre, si impegna a divulgare il documento di *e-Safety Policy*.

## 3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE TIC DELLA SCUOLA.

L'infrastruttura e la strumentazione TIC dell'Istituto sono un patrimonio di tutti e vanno utilizzate nel rispetto delle norme contenute nella Procedura 14 - *Accesso e utilizzo delle postazioni multimediali*.

I danni causati alle attrezzature saranno a carico dei singoli responsabili e/o di chi ne fa le veci, in caso di utenti minorenni, e di chiunque disattenda il suddetto Regolamento.

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

L'Istituto è dotato di una rete wireless nella maggior parte dei plessi. Tutti gli accessi sono dotati di filtri antivirus e di limitazioni per una sicura e corretta navigazione.

L'accesso a infrastruttura e strumentazione TIC è riservato a scopi didattici o amministrativi.

### 3.2 GESTIONE ACCESSI (PASSWORD, BACKUP, ECC.)

L'accesso a internet è consentito a scopi didattici al personale docente attraverso l'assegnazione di una password comune. Agli alunni è permessa la navigazione in internet dai pc del laboratorio o delle aule collegate alle LIM sotto il diretto controllo dei docenti, che non possono comunicare la chiave di accesso, salvo diversa autorizzazione.

L'accesso a internet è consentito al personale di segreteria attraverso l'assegnazione di una password comune a tutti, per le necessità di istituto; gli stessi operatori non devono mai comunicare la password di accesso.

Allo stato attuale non vi è un backup dei file elaborati, se non quello operato dai docenti e dagli alunni interessati sui supporti rimovibili personali. Le postazioni del laboratorio funzionano come stazioni di lavoro e anche come archivi.

### 3.3 E-MAIL.

L'account di posta elettronica istituzionale della scuola è quello fornito dal Ministero dell'Istruzione dell'Università e della Ricerca, sia nella versione posta ordinaria che certificata. Questi account sono utilizzati ordinariamente ed esclusivamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita: l'invio o la ricezione di posta a scopi didattici avviene su autorizzazione del DS e operativamente è svolto dall'assistente amministrativo addetto.

Ogni dipendente è dotato di posta elettronica personale tale sistema è l'unico ad oggi possibile per lo scambio di informazioni tra docenti, al condivisione di dati anonimi.

In futuro si prevede di implementare un sistema di posta elettronica per ogni dipendente sul dominio dell'istituto. In questo caso le caselle di posta elettronica saranno di tipo "aziendale" e non potranno essere utilizzate per scopi personali. Saranno attivati gruppi di discussione per ordine di scuola e per plesso. La funzionalità dei gruppi di discussione servirà per consentire un rapido scambio di informazioni, opinioni, documenti tra colleghi e incentivare la partecipazione di tutti i docenti alla vita scolastica. La policy di uso della casella di posta elettronica sarà dettagliatamente pubblicata sul sito dell'Istituto nella sezione "note legali".

Le circolari, le informazioni principali, le convocazioni sono attualmente diramate nella bacheca del registro elettronico e tramite posta elettronica.

### 3.4 SITO WEB DELLA SCUOLA.

La scuola attualmente ha un sito web. Tutti i contenuti del settore didattico sono pubblicati sotto supervisione della Funzione Strumentale, che ne valuta con il DS la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy.

### 3.5 SOCIAL NETWORK.

A partire dall' a.s. 2018/2019 la scuola, sulla base di un progetto PON, aprirà una pagina Facebook per la condivisione di buone pratiche per stimolare la lettura critica della realtà.

### 3.6 CLOUD STORAGE

I docenti si avvalgono allo stato attuale di alcuni software di cloud storage per condividere materiale didattico (ad esempio Google Drive). La possibilità di utilizzare in futuro un server interno alla scuola potrà fare modificare questa pratica.

### 3.7 REGISTRO ELETTRONICO.

Ogni famiglia degli studenti di scuola Secondaria di primo grado riceve le credenziali per l'accesso riservato al registro elettronico, in cui il corpo docente è tenuto a registrare assenze, valutazioni, note e osservazioni. Tramite le stesse credenziali i genitori possono controllare assenze, valutazioni, note e osservazioni.

### 3.8 PROTEZIONE DEI DATI PERSONALI.

Il personale scolastico è incaricato del trattamento dei dati personali (degli alunni, dei genitori, ecc.), necessari ai fini dello svolgimento della propria funzione e nello specifico per la docenza (istruzione e formazione). Tutto il personale incaricato riceve istruzioni particolareggiate applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi.
Il responsabile del trattamento e dell'archiviazione dei dati sensibili sarà individuato dal DS.
Viene inoltre fornita, volta per volta, ai genitori l'informativa e la richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori. All'atto dell'iscrizione è altresì richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico di immagini e video dei minori per la documentazione delle attività didattiche.

## 4. STRUMENTAZIONE PERSONALE

Premesso che l'IC "Garibaldi" di Chiavenna possiede e dà in uso gratuito, durante le ore di lezione, agli alunni con bisogni educativi speciali, dei computer portatili, collegati se necessario al sistema Wi-Fi della scuola, l'uso di computer personali andrà implementato attraverso una regolamentazione del BYOD (*Bring Your Own Device*) in raccordo con il Regolamento d'istituto.
Si rammenta, inoltre, ai sensi della Direttiva Ministeriale n. 30 del 15 marzo 2007, che con la condivisione della presente Policy, le famiglie si assumono l'impegno di rispondere direttamente dell'operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone a seguito di violazioni della presente Policy.
Si ribadiscono le seguenti raccomandazioni generali prescrittive:

- la scuola consiglia vivamente a tutti gli studenti di non portare telefoni cellulari e dispositivi mobili personali;
- per le scuole primarie si vieta ai genitori la possibilità di far portare a scuola ai loro bambini il telefono cellulare/tablet se non in casi speciali e concordati con il corpo docente che ne delibera l'uso (quando, come, perché, per quanto tempo);
- per la scuola dell'infanzia il divieto è categorico. In generale

### 4.1 Per gli studenti:

I telefoni cellulari e i tablet, le fotocamere/videocamere e i registratori vocali, le schede o le memorie di archiviazione di massa esterne non possono essere

utilizzati durante le attività scolastiche del mattino (compreso gli intervalli) e del pomeriggio (siano esse facoltative o obbligatorie) in tutti gli ambienti scolastici.
Qualora gli alunni utilizzino a scuola le schede o le memorie di archiviazione di massa esterne di proprietà personale, all'interno di attività didattiche espressamente programmate e con il permesso dei docenti, le stesse devono essere preventivamente controllate tramite i software della rete scolastica al fine di accertare la presenza di virus, malware, spyware, ecc., che possano danneggiare le attrezzature comuni.
I dispositivi devono essere tenuti spenti e opportunamente custoditi e depositati nei borsoni, zaini, giacche: mai sul banco né tra le mani. I dispositivi possono essere utilizzati previa autorizzazione dei docenti nel corso di viaggi e uscite d'istruzione per documentare le attività didattiche. In occasione dei viaggi d'istruzione che richiedono il pernottamento i consigli di classe stabiliscono gli orari d'uso dei cellulari e le modalità di riconsegna ai docenti accompagnatori nelle ore notturne.
La scuola non è responsabile della custodia e dei danneggiamenti che tali strumenti possono subire.
Telefoni e dispositivi non devono mai essere usati durante le verifiche scritte, durante gli esami e le prove nazionali.
Tali norme hanno valore sia per gli alunni della scuola primaria, sia per quelli della scuola secondaria di primo grado.
Per gli alunni con disabilità, con disturbi specifici di apprendimento, BES, previa consultazione con il consiglio di Classe, i genitori e gli operatori sanitari concorderanno le modalità di uso degli strumenti compensativi, sia per quelli forniti dall'IC "Garibaldi" di Chiavenna, sia per quelli personali. A tal proposito si rammenta che la copertura assicurativa comprende solo il danneggiamento per i dispositivi indispensabili all'attività didattica degli studenti con disabilità.
All'interno di tutti i locali della scuola sono vietate riprese audio e video di ambienti e persone, salvo in caso di esplicita autorizzazione del docente responsabile per attività didattiche.
La pubblicazione in rete di immagini e/o video ripresi all'interno dell'Istituto è vietata.
Si ricorda che, secondo la normativa vigente, non si possono diffondere immagini, video o foto sul web.
La legge 71/2017, in materia di prevenzione al cyber bullismo, ci ricorda che la pubblicazione di immagini, video e riprese non autorizzate possono rientrare nella fattispecie dei reati ascrivibili al fenomeno e quindi perseguibili.
In caso di violazione delle sopra individuate disposizioni, si darà seguito a quanto previsto nell'apposito punto del Regolamento dell'Istituto.
Le comunicazioni tra alunni e famiglia durante l'orario scolastico, devono passare esclusivamente tramite gli apparecchi telefonici della scuola sia in ingresso che in uscita. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.

4.2 Per il personale docente:

Il personale docente utilizza le infrastrutture, le connessioni e la strumentazione fornita dalla scuola esclusivamente per fini didattici e professionali.

Tutti i docenti sono autorizzati ad utilizzare dispositivi personali:

- laddove non stiano assolvendo ad un ruolo didattico, a condizione che l'utilizzo non intralci il normale svolgimento delle attività scolastiche, né distragga dal corretto svolgimento delle proprie mansioni;
- nello svolgimento di attività didattiche esterne ai plessi scolastici;
- durante le lezioni scolastiche all'interno di attività didattiche espressamente programmate;
- nel caso di blocchi del sistema informatico della scuola e fino alla riparazione dei guasti.

La scuola non è responsabile della custodia e dei danneggiamenti che tali strumenti possono subire, pertanto la responsabilità sulla conservazione e corretta gestione degli stessi è affidata unicamente al docente proprietario.

Le password di accesso ai computer ed alla rete wireless della scuola vanno custodite con cura ed è vietato divulgarle a chi non ha titolo per utilizzarla (studenti, genitori, operatori esterni).

Qualora i docenti utilizzino a scuola le schede o le memorie di archiviazione di massa esterne di proprietà personale le stesse devono essere preventivamente controllate tramite i software della rete scolastica al fine di accertare la presenza di virus, malware, spyware, ecc., che possano danneggiare le attrezzature comuni.

L'archiviazione degli elaborati dei docenti avverrà esclusivamente sul computer della classe o su quelli presenti in aula insegnati, in directory indicanti la classe, l'anno scolastico e le cartelle personali con il nome del docente e la materia.

L'archiviazione dei dati sensibili e riservati è vietata su ogni computer ad eccezione di quello a disposizione delle segreterie e dei docenti di sostegno, coperti da password riservate al solo uso del personale addetto.

4.3 Per il personale non docente:

Il personale ATA utilizza le infrastrutture, le connessioni e la strumentazione fornita dalla scuola esclusivamente per fini professionali.

Tutti gli operatori sono autorizzati ad utilizzare dispositivi personali:

- laddove non stiano assolvendo ad un ruolo istituzionale, a condizione che l'utilizzo non intralci il normale svolgimento delle attività, né distragga dal corretto svolgimento delle proprie mansioni;
- nello svolgimento di ausilio alle attività didattiche esterne ai plessi scolastici;
- nel caso di blocchi del sistema informatico della scuola e fino alla riparazione dei guasti.

La scuola non è responsabile della custodia e dei danneggiamenti che tali strumenti possono subire, pertanto la responsabilità sulla conservazione e corretta gestione degli stessi è affidata unicamente all'operatore proprietario.

Le password di accesso ai computer ed alla rete wireless della scuola vanno custodite con cura ed è vietato divulgarle a chi non ha titolo per utilizzarla (studenti, genitori, operatori esterni).

Qualora gli operatori utilizzino a scuola le schede o le memorie di archiviazione di massa esterne di proprietà personale le stesse devono essere preventivamente controllate tramite i software della rete scolastica al fine di accertare la presenza di virus, malware, spyware, che possano danneggiare le attrezzature comuni.

L'archiviazione degli elaborati degli operatori avverrà esclusivamente sui computer della segreteria, in directory indicanti in modo chiaro l'argomento e l'anno scolastico e cartelle personali con il nome dell'operatore.

## 5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

### 5.1 PREVENZIONE

Per gli studenti nativi digitali le interconnessioni tra vita e tecnologia sono la normalità. Essi, pur essendo spesso tecnicamente competenti, tendono a non cogliere le implicazioni dei loro comportamenti. Tale fenomeno è tanto maggiore quanto è più forte il coinvolgimento emotivo nell'utilizzo dei nuovi media.

Ciò fa sì che alcuni rischi che fanno parte del mondo digitale possano non essere percepiti come tali ed è dunque compito degli adulti, famiglie ed insegnanti, affrontarli con l'obiettivo di prevenirli. L'istituto è impegnato in iniziative volte a promuovere la cultura dell'inclusione, del rispetto dell'altro e delle differenze, nonché l'utilizzo consapevole, positivo e responsabile delle Tecnologie dell'Informazione e della Comunicazione (TIC).

A tal fine è responsabilità di ciascun docente cogliere ogni opportunità per riflettere insieme agli alunni sui rischi in oggetto, nonché monitorare costantemente le relazioni interne alla classe, onde individuare possibili situazioni di disagio ed intervenire tempestivamente, anche mediante il ricorso a figure di sistema preposte (psicopedagogista d'istituto), per sostenere il singolo nelle situazioni di difficoltà personale e indirizzare il gruppo verso l'instaurazione di un clima positivo, di reciproca accettazione e rispetto, nelle situazioni di difficoltà socio-relazionale.

Tale percorso interno è ulteriormente rinforzato dalla partecipazione a progetti e/o iniziative di formazione dei docenti, coerenti con i temi sopra menzionati, cui la scuola pone particolare attenzione. La scuola si avvale della collaborazione di enti, associazioni e delle forze dell'ordine per realizzare incontri rivolti ad alunni, docenti e genitori con l'intento di fornire ogni elemento utile alla prevenzione, alla gestione dei problemi relativi alla sicurezza informatica e l'uso delle TIC nella didattica.

#### 5.1.1. RISCHI

Tra i principali rischi, sia di carattere comportamentale, che di matrice tecnica, ricordiamo:

- possibile esposizione a contenuti dannosi e non adatti alla loro età;
- videogiochi diseducativi;
- pubblicità ingannevoli;
- accesso ad informazioni scorrette;
- virus informatici in grado di infettare computer e cellulari;
- possibili contatti con adulti che vogliono conoscere e avvicinare bambini/e o ragazzi/e (adescamento);
- cyber-bullismo;
- scambio di materiale a sfondo sessuale (sexting);
- uso eccessivo di Internet/cellulare (dipendenza).

#### 5.1.2. AZIONI

Verso gli studenti:

- Inserimento nel curricolo di temi legati ai pericoli di internet, all'affidabilità delle fonti online, all'interculturalità e al rispetto delle diversità.
- Sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni.
- Campagne di sensibilizzazione e informazione anche con l'ausilio di progetti di enti esterni sul cyberbullismo.
- Sensibilizzazione e informazioni sulla dipendenza da Internet (videogiochi, shopping, ecc.) e sul fatto che ciò può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito ad

insaputa di altri) rappresenta un vero e proprio illecito.
Verso i genitori:
Informazione circa le possibilità di attivare forme di controllo parentale della navigazione e sensibilizzazione sulla necessità di monitorare l'esperienza online dei propri figli.

## 5.2 RILEVAZIONE

**La rilevazione dei casi è compito dell'intera comunità educante**. Familiari, tutori, docenti e personale ATA sono invitati a essere confidenti e custodi, diretti o indiretti, di ciò che gli studenti vivono: si raccomanda di assumere atteggiamenti di ascolto per riuscire a ricevere dai minori più fragili segnalazioni e confidenze circa situazioni problematiche vissute.
I docenti in particolare sono chiamati a essere attenti alle problematiche, ai rischi, ai pericoli che gli studenti possono vivere e affrontare ogni giorno. Accorgersi tempestivamente di quanto accade e compiere azioni immediate di contrasto verso gli atti inopportuni – quando non illegali - diviene fondamentale per poter evitare conseguenze a lungo termine che possano pregiudicare il benessere e una crescita armonica dei soggetti coinvolti.
Laddove il docente colga possibili situazioni di disagio connesse ad uno o più di uno tra i rischi elencati nel paragrafo “Prevenzione”, dovrà segnalare il caso e potrà chiedere il supporto del Consiglio di Classe, degli operatori dello sportello d’ascolto, del Referente per la prevenzione del cyberbullismo, del Dirigente Scolastico.
Il docente in ogni caso avrà cura di compilare la “scheda di segnalazione” sotto riportata.

## 5.3 GESTIONE DEI CASI

Come previsto nel Regolamento d’istituto, a seguito della segnalazione, verrà avviato un colloquio tra le componenti scolastiche sopra elencate, finalizzato a valutare la necessità di effettuare uno o più interventi di osservazione in classe e, successivamente, di pianificare adeguati interventi educativi e, ove necessario, di coinvolgere le famiglie per l’attivazione di un percorso comune e condiviso di sostegno al disagio. Le azioni poste in essere dalla scuola saranno dirette non solo a supportare le vittime, le famiglie e tutti coloro che sono stati spettatori attivi o passivi di quanto avvenuto, ma anche a realizzare interventi educativi rispetto a quanti abbiano messo in atto comportamenti lesivi, ove si tratti di soggetti interni all’Istituto. Nei casi di maggiore gravità si valuterà anche il coinvolgimento di attori esterni quali le forze dell’ordine e i servizi sociali.

AZIONI DA INTRAPRENDERE A SECONDA DELLA SPECIFICA DEL CASO:

| RILEVAZIONE DEL CASO | AZIONI |
|---|---|
| Utilizzo del telefono cellulare e dei vari dispositivi elettronici (lettori mp3, ipod, ipad, notebook, fotocamera, videocamera, ecc…) durante le attività scolastiche del mattino (compreso gli intervalli) e del pomeriggio (obbligatorie e facoltative). | Ogni segnalazione verrà valutata dal Ds e dalla Referente che attiveranno a seconda della gravità dei fatti procedure di sanzione/accompagnamento con eventuale coinvolgimento degli organi collegiali anche in accordo alla normativa sulla privacy. |
| Violazione della privacy, attraverso raccolta e uso delle immagini, filmati e riprese sonore non autorizzati; | Ogni segnalazione verrà valutata dal Ds e dalla Referente che attiveranno a seconda della gravità dei fatti procedure di sanzione/accompagnamento con eventuale coinvolgimento degli organi collegiali in accordo alla normativa sulla privacy. |
| Per atti di cyber bullismo, quali: – flaming (litigi on line con uso di linguaggio violento e volgare); – cyberstalking; – denigrazione (pubblicazione all'interno di comunità virtuali, quali blog, newsgroup, messaggistica immediata, profili face book, di pettegolezzi e commenti crudeli, calunniosi e denigratori; – esclusione (estromissione intenzionale dall'attività on line); – sexting (invio di messaggi via smartphone o internet, corredatti da immagini a sfondo sessuali) | Ogni segnalazione verrà valutata dal Ds e dalla Referente che attiveranno a seconda della gravità dei fatti procedure di sanzione/accompagnamento con eventuale coinvolgimento degli organi collegiali in accordo alla normativa sulla privacy. |

In base alle nuove disposizioni della L 71/2017, confermate dalle linee di orientamento del MIUR dell'ottobre 2017, qualora nella scuola vengano segnalati atti di bullismo e cyber bullismo, che non si configurino come reati, il Dirigente Scolastico deve informare chi esercita la responsabilità genitoriale/tutore/affidatario dei minori coinvolti (o chi ne esercita la responsabilità o chi esercita la responsabilità genitoriale/tutore/affidatario).