ISTITUTO COMPRENSIVO STATALE "ERNESTO PUXEDDU"
CAIC840003 - VIA PORRINO, 12 – 09034 VILLASOR
TEL. 070 9648045 – C.F. 91013590921 – CODICE UFFICIO: UF5IWW
E-MAIL: CAIC840003@ISTRUZIONE.IT – PEC: CAIC840003@PEC.ISTRUZIONE.IT
SITO WEB: WWW.ISTITUTOCOMPRENSIVOVILLASOR.EDU.IT

E-SAFETY POLICY

A.S. 2023/24

Allegato n. 2 al Regolamento di istituto

1. Introduzione

1.1 Scopo della E-Policy

Lo scopo del presente documento, Policy di e-safety, è quello di informare tutta l'utenza di codesto Istituto sull'utilizzo corretto e responsabile degli strumenti informatici collegati alla rete scolastica, attraverso la presentazione delle linee guida di questa Scuola in merito all'utilizzo delle tecnologie dell'informazione, oggi indispensabili anche in ambito didattico.
Tutti i membri di questa comunità scolastica, minori e non, dovranno essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete: entrare accidentalmente in contatto con materiale inadeguato e/o illegale, quando si è online, è una possibilità non remota, pertanto, la scuola e gli insegnanti indicano le giuste regole di condotta per un uso critico e consapevole di Internet e promuovono l'adozione di strategie che prevengano il verificarsi di situazioni potenzialmente pericolose. La Policy di e-safety permette di regolare il comportamento degli alunni dentro le aule scolastiche e di sensibilizzarli all'adozione di buone pratiche quando sono fuori dalla scuola e autorizza i membri del personale docente a erogare sanzioni disciplinari per comportamenti inappropriati avvenuti all'interno dell'istituzione scolastica, infatti, opportune azioni disciplinari saranno intraprese nel caso di comportamenti inappropriati o addirittura illeciti.

1.2 Ruoli e Responsabilità

Il **Dirigente Scolastico** è responsabile per la sicurezza dei dati, è informato sulle linee guida contenute nella e-policy ed è garante della sua applicazione. I suoi compiti sono:

- garantire la sicurezza online dei membri della comunità scolastica;
- garantire che tutti gli insegnanti ricevano una formazione adeguata che consenta loro di promuovere 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;
- comprendere e seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.

Il **referente per il Cyber-bullismo** si assicurerà che i contenuti della presente e-policy vengano diffusi a tutti gli utenti della scuola, cogliendo ogni occasione per sensibilizzare docenti e genitori circa i rischi legati alla rete, attraverso incontri con la Polizia Postale e/o altri esperti o educatori, circolari, sito web e altre comunicazioni telematiche, informazioni su campagne di sicurezza promosse da altre istituzioni o su convegni dedicati a questo tema

L'animatore Digitale ed il Team dell'innovazione digitale (con l'ausilio del referente al cyber-bullismo) si occuperanno di:

- pubblicare la policy sul sito della scuola stimolare la formazione interna all'istituzione 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;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate;
- coinvolgere alunni, genitori e altri attori del territorio, nella partecipazione ad attività e progetti attinenti la "scuola digitale".

Gli **insegnanti** inseriscono tematiche legate alla sicurezza online nella didattica e guidano gli alunni nelle attività che prevedono l'accesso alla rete. In particolare, i loro compiti consistono nel:

- 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;
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti idonei ad un utilizzo scolastico/didattico, nonché controllare l'uso delle tecnologie digitali, dispositivi mobili,

macchine fotografiche ecc. nelle lezioni e nelle altre attività scolastiche che ne prevedono la necessità a scopi didattici;
- comunicare ai genitori difficoltà, bisogni o disagi rilevati dagli alunni a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- 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.

Gli **alunni** conoscono e rispettano i regolamenti (generali e specifici delle aule di informatica) e segnalano al docente di classe eventuali usi impropri della rete e dei dispositivi. 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 di studio, ricerca ed approfondimento;
- comprendere l'importanza di adottare buone pratiche di sicurezza online 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.

I **genitori** sostengono la scuola nel promuovere la sicurezza online, leggendo la policy e partecipando agli incontri organizzati dalla scuola sui temi della sicurezza online. Il ruolo dei genitori 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;
- seguire i figli nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di internet, anche nei dispositivi mobili (cellulari e tablet);
- fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e del proprio cellulare.

Si specifica che in caso di violazione del Regolamento d'Istituto nella parte che recita "Riprendere e/o diffondere in rete immagini e/o video e/o diffondere testi con riferimenti personali su altre persone, appartenenti alla comunità scolastica senza autorizzazione dell'interessato" (vedasi art. 22 pag. 15) **la responsabilità relativa alla violazione delle norme di cui al G.D.P.R. 2016 - REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 – da parte del minore, che ricade sull'esercente la patria potestà, è di natura penale**.

In considerazione della fascia di età degli alunni, alcune azioni da parte dei genitori potrebbero favorire un uso poco corretto e responsabile delle TIC da parte dei figli anche a scuola. Le situazioni familiari meno favorevoli al corretto utilizzo sono:
- consentire al proprio figlio piena autonomia nella navigazione sul web e nell'utilizzo dello smartphone;
- non vigilare sul proprio figlio mentre utilizza pc, tablet o cellulare.

1.3 Condivisione e comunicazione della Policy all'intera comunità scolastica

La E-Policy è pubblicata sulla Home Page del sito della scuola dopo essere stata approvata dal Collegio dei Docenti. All'inizio di ogni anno scolastico, insieme al Patto di Corresponsabilità Educativa, la E-Policy verrà illustrata ai genitori e agli alunni.

1.4 Gestione delle infrazioni alla Policy

Nel caso in cui un docente rilevi un'infrazione alle indicazioni della Policy è necessario che informi il coordinatore di classe, il quale a sua volta riferisce al Dirigente Scolastico e alla famiglia.

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali di internet sono:

- un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;
- l'invio non autorizzato di foto o di altri dati personali come l'indirizzo di casa o il telefono;
- la condivisione di immagini intime;
- la comunicazione incauta e senza permesso con sconosciuti;
- il collegamento a siti web non espressamente indicati dai docenti e potenzialmente pericolosi.

Gli interventi correttivi previsti per gli alunni sono coerenti con quanto definito nel Regolamento d'istituto. Nel caso in cui l'infrazione si configuri come atto di cyber-bullismo, il docente informa il referente per il bullismo/cyber-bullismo. Nel caso si tratti di un reato è necessario che il Dirigente informi le autorità competenti (polizia postale).
I genitori degli alunni possono essere convocati a scuola per concordare le misure educative più appropriate 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.
Le potenziali infrazioni a carico del personale scolastico sono identificabili in:

- trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- diffusione delle password assegnate per la navigazione online attraverso la rete della scuola.

1.5 Monitoraggio dell'implementazione della Policy e suo aggiornamento

Il Dirigente Scolastico è responsabile dell'implementazione della Policy all'interno dell'Istituto. L'Animatore Digitale (insieme al Team dell'innovazione digitale) e il Referente per il Bullismo e il Cyber-bullismo, in accordo con il Dirigente Scolastico, partecipano alla revisione e all'aggiornamento del documento che dovrà sempre essere sottoposto all'approvazione del Collegio dei Docenti.

1.6 Integrazione della Policy con Regolamenti esistenti

Il presente documento si integra pienamente per obiettivi e contenuti con il PTOF, incluso il piano per l'attuazione del PNSD, con il Regolamento Interno di Istituto e con il Patto di Corresponsabilità.

2. Formazione e curricolo

2.1 Curricolo sulle competenze digitali per gli studenti

Possedere competenze digitali significa padroneggiare le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con "autonomia e responsabilità" nel rispetto degli altri e sapendone prevenire i pericoli. L'impiego delle TIC è senz'altro un fattore di innovazione della didattica e di aumento della motivazione degli studenti. Tuttavia non è sufficiente possedere la dotazione tecnologica, ma è fondamentale la capacità di comprenderne le potenzialità rispetto a contesti e finalità specifiche. Un alunno competente dal punto di vista digitale sarà colui che non solo possiede abilità informatiche di base, come conoscere specifici software o servizi web, ma saprà ricercare e selezionare le informazioni più utili online, saprà lavorare in maniera collaborativa, anche a distanza, saprà tutelare la propria privacy nella rete e nei social network in particolare, saprà sfruttare la tecnologia in maniera consapevole, critica e creativa, per costruire conoscenza.
Le competenze digitali vengono promosse in maniera trasversale dai docenti, sulla base delle loro pratiche di insegnamento, in modo tale da:

- insegnare ciò che è accettabile nell'utilizzo di Internet e ciò che è vietato, fornendo strumenti per l'utilizzo efficace di Internet e la conoscenza delle conseguenze delle violazioni;
- mostrare come produrre, pubblicare e presentare contenuti digitali in modo appropriato, sia in ambienti privati sia per un pubblico più vasto;
- insegnare la valutazione dell'attendibilità dei contenuti Internet.

L' alunno, al termine del primo ciclo di istruzione:

- (al termine della scuola primaria) utilizza le Tecnologie dell'informazione e della Comunicazione (TIC) per ricercare informazioni a supporto della sua attività di studio e produce, tramite le TIC, relazioni e presentazioni relative ad argomenti di studio;
- (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.

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

La formazione è in parte lasciata all'iniziativa dei singoli docenti, in parte offerta dalla scuola secondo le varie proposte che pervengono al e dal Dirigente Scolastico. La scuola assicura tempestiva e capillare informazione su corsi, convegni e seminari che riguardino tali argomenti, cercando di agevolare il personale che intenda parteciparvi. Infine, la scuola può aderire a progetti appositi di formazione presentati da enti e associazioni, come già avvenuto in passato.

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

Anche il percorso della formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet, può prevedere momenti di autoaggiornamento e momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie.
Nel sito della scuola è presente materiale fruibile dai docenti per l'aggiornamento sull'utilizzo consapevole e sicuro di internet, nonché il link al sito "Generazioni connesse".

2.4 Sensibilizzazione delle famiglie

L'Istituto, attraverso la figura dell'Animatore Digitale e del referente per il cyber-bullismo, attiverà iniziative per sensibilizzare le famiglie all'uso consapevole della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. In particolare, verrà messo a disposizione dei genitori del materiale informativo su tali tematiche, anche rimandando a siti specializzati e delle forze dell'ordine.
La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento (Policy e-safety) per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e prevenire i rischi legati a un utilizzo non corretto di internet.
A partire dalla scuola primaria, questo Istituto invita i genitori ad assumersi l'incarico di accompagnare e supervisionare i figli durante la navigazione in rete, aiutandoli a riconoscere ed evitare i rischi. I docenti suggeriscono la consultazione del portale **Generazioni Connesse**, dotato di una specifica Area Genitori, dove è possibile reperire informazioni e consigli pratici per una equilibrata e consapevole gestione del rapporto tra bambini, ragazzi e media. Nel portale sopracitato sono presenti materiali dedicati ad alunni (per diverse fasce di età) e alle famiglie come guide in formato .pdf e video che possono fornire spunti di approfondimento e confronto.

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

3.1 Accesso ad internet: filtri, antivirus e sulla navigazione

Tutte le aule della scuola secondaria e primaria dell'Istituto sono dotate di una infrastruttura informatica completa (server Qubiarch) che provvede a monitorare il traffico web nelle diverse postazioni dei dispositivi connessi ai pannelli interattivi (thin client) delle aule didattiche e dell'aula di informatica, aggiornare gli antivirus e bloccare l'accesso a siti inappropriati al contesto scolastico, garantendo un discreto livello di sicurezza online. La scuola è in possesso di chromebook, pc e tablet, ognuno dei quali è dotato di un proprio codice identificativo, è protetto da filtri appositi e si collega o al modem portatile dedicato alla didattica o alle reti wi-fi scolastiche solo attraverso password che i docenti di volta in volta inseriscono e non rendono note agli alunni.

3.2 Gestione accessi

Tutte le aule sono dotate di terminali collegati alla piattaforma Qubiarch a disposizione dei docenti per la compilazione del registro elettronico e come supporto alla didattica. Questi terminali sono protetti da password personali riservate ai docenti.
I computer del laboratorio linguistico della scuola secondaria di Villasor possono essere utilizzati solo sotto stretta vigilanza (da parte dei docenti di lingue straniere) con uso esclusivo del software Nibelung.
La connessione alla rete wi-fi è riservata agli insegnanti per fini didattici ed è possibile accedervi solo attraverso una password.

3.3 Sito web della scuola

Il sito dell'Istituto Comprensivo è raggiungibile all'indirizzo: **www.istitutocomprensivovillasor.edu.it**
Il Dirigente e lo staff incaricato verificano i contenuti destinati alla pubblicazione.

3.4 Social network

Tutte le classi hanno la possibilità di utilizzare le classi virtuali della piattaforma Workspace di Google e di utilizzare gli strumenti della piattaforma che hanno a disposizione. Gli alunni accedono alla piattaforma grazie alle credenziali fornite dalla segreteria al momento dell'iscrizione.

3.5 Protezione dei dati personali

In fase di iscrizione degli alunni al nostro istituto, i genitori rilasciano il consenso all'utilizzo di materiale fotografico e audiovisivo per pubblicazioni in formato cartaceo e/o digitale all'interno dell'edificio scolastico e/o nel sito della scuola, e nelle piattaforme didattiche in uso (Google Workspace).
L'accesso ai dati di ogni singolo alunno, riportati nel registro elettronico (ritardi, assenze, note disciplinari, richiami, annotazioni e valutazioni), è riservato ai rispettivi genitori tramite l'invio di una password di accesso strettamente personale.

4. Strumentazione personale

Per gli studenti di codesto Istituto è vietato l'utilizzo di cellulari per l'intera durata delle attività scolastiche, inclusi gli intervalli, a meno che non venga esplicitamente consentito dal docente, per fini strettamente didattici o in casi di urgenza.
Il telefono cellulare non è richiesto dalla scuola perché non è ritenuto indispensabile in ambito scolastico, ma viene fornito dai genitori degli alunni al fine di comunicare direttamente con i figli anche fuori dal contesto scolastico.
È vietato agli alunni usare dispositivi di registrazione audio, videocamere o fotocamere per registrare media o fare foto in classe senza il permesso dell'insegnante e senza il consenso della persona che viene registrata.
È consentito a tutti gli alunni, in casi specifici concordati con il docente (uscite didattiche, produzioni multimediali...) l'utilizzo di dispositivi elettronici personali per scopi didattici.

5. Prevenzione, rilevazione e gestione dei casi

5.1 Prevenzione

5.1.1 Rischi

I rischi effettivi che si possono correre a scuola nell'utilizzo delle TIC da parte degli alunni derivano da un uso non corretto dello smartphone o dei pc della scuola collegati alla rete.
Eludendo la sorveglianza degli insegnanti, attraverso gli smartphone, dotati di collegamento a internet, gli alunni potrebbero anche scaricare e spedire foto personali o intime, proprie o di altri, video con contenuti indecenti o violenti, accedere a internet e a siti non adatti ai minori, ascoltare musica e giocare con i videogiochi non adeguati ai minori, leggere la posta elettronica e comunicare o chattare

con sconosciuti, inviare o ricevere messaggi molesti e minacciosi. Eludendo sempre la vigilanza degli insegnanti, gli alunni potrebbero correre gli stessi rischi a scuola anche con l'utilizzo dei pc non collegati a Qubiarch.

5.1.2 Azioni

Le azioni previste, di prevenzione nell'utilizzo delle TIC, sono le seguenti:

- Informare e formare i docenti, i genitori, il personale ATA e gli studenti sui rischi che un uso non sicuro delle nuove tecnologie può favorire;
- Non consentire l'utilizzo del cellulare personale degli alunni a scuola (nella scuola secondaria di Villasor, all'ingresso il dispositivo andrà depositato nell'armadietto personale, che ogni singolo alunno potrà chiudere a chiave). Per assolvere a ogni comunicazione urgente con i genitori o con chi ne fa le veci è sempre disponibile il telefono della scuola supervisionato dai collaboratori scolastici, che prima di passare la telefonata al discente si accertano dell'identità dell'interlocutore;
- Consentire l'utilizzo del cellulare solo in casi particolari ed eccezionali, ad esempio quando ci si trova fuori dal contesto scolastico durante una visita guidata, e comunque sotto la supervisione dell'insegnante, che si accerta preventivamente dell'identità dell'interlocutore;
- Consentire l'utilizzo di visori VR sotto stretta sorveglianza del docente per attività didattiche di breve durata e previa autorizzazione del genitore;
- Utilizzare filtri e/o software che impediscono il collegamento ai siti web per adulti.

La scuola si impegna ad attrezzare le aule con dispositivi elettronici sicuri e protetti.
I docenti si impegnano ad organizzare per gli alunni momenti di riflessione sui temi dell'utilizzo consapevole di internet e a formarsi su queste tematiche.
I genitori si impegnano a prendere visione della E-safety Policy e a seguire le azioni promosse dalla scuola per l'utilizzo consapevole della rete.
Gli alunni si impegnano a rispettare i regolamenti e a partecipare attivamente alle occasioni di confronto su queste tematiche organizzate dalla scuola.
Per i rischi connessi all'utilizzo delle nuove tecnologie (grooming o adescamento online, cyberbullismo, furto di identità e sexting), la scuola si affida a consulenti esterni per organizzare incontri informativi rivolti agli alunni.
In questo documento si intende ricordare agli utenti dell'Istituto che la scuola è un'istituzione educativa e che non è né prevista, né possibile, né tantomeno legittima la perquisizione quotidiana di tutti gli studenti all'inizio di ogni giorno di lezione. Per questo motivo, le responsabilità che dovessero derivare dal verificarsi di eventi riconducibili all'uso non corretto o non legittimo del proprio cellulare e/o tablet sono tutte ascrivibili alle famiglie degli studenti eventualmente coinvolti.
Le responsabilità appena menzionate sono ascrivibili al personale scolastico solo se, dopo aver personalmente constatato il possesso, durante l'orario scolastico, di uno smartphone da parte degli alunni, non dovesse immediatamente intervenire nelle forme indicate qui e nel Regolamento di Istituto e comunque in modo tale da prevenire o reprimere sul nascere situazioni potenzialmente rischiose.

5.2 Rilevazione

5.2.1 Che cosa segnalare

Si considerano da segnalare tutte quelle situazioni che si configurano come episodi di cyber-bullismo (caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona o un piccolo gruppo tramite un utilizzo irresponsabile dei social network), ma anche usi inappropriati della rete (siti d'odio, contenuti non adatti all'età degli alunni...). Più in dettaglio, i contenuti "pericolosi" comunicati/ricevuti a/da altri, messi/scaricati in rete per gli alunni possono essere i seguenti:

- contenuti afferenti alla privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);

- contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);
- contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia).

5.2.2 Come segnalare: quali strumenti e a chi

I docenti di classe, (attraverso apposito modulo di segnalazione), informano il referente per il bullismo/cyber-bullismo e il coordinatore di classe. Il referente a sua volta inoltra la segnalazione al Dirigente Scolastico, il quale procede ad informare le famiglie. Tutte le segnalazioni riportate dai docenti vengono annotate sul registro elettronico in apposita sezione:
-convocazione della famiglia affinché venga messa al corrente dell'accaduto e stesura di un verbale controfirmato dai genitori;
- nota disciplinare o richiamo, visibile ai docenti del Consiglio di Classe e famiglia dell'alunno.
Qualora ci si dovesse accorgere che l'alunno, usando il computer, si sta servendo di un servizio di messaggistica istantanea, programma che permette di chattare in linea tramite testo, l'insegnante può copiare, incollare e stampare la conversazione. Per gli eventuali collegamenti non autorizzati a siti social network e altri website, l'insegnante può conservare il link, stampare la pagina o salvare la schermata su documento word.
Per le e-mail si può stampare la mail o conservare l'intero messaggio, compresa l'intestazione del mittente.
Gli insegnanti, anche con l'ausilio tecnico dell'Animatore digitale, possono provvedere a conservare tutte le prove di una condotta scorretta o incauta rilevate sui pc della scuola: soprattutto la data e l'ora, il contenuto di eventuali messaggi spediti o l'indirizzo web del sito visitato.

5.2.3 Come gestire le segnalazioni

Se le prove di un uso scorretto delle tic o del web non dovessero essere disponibili ma si avessero a disposizione solo le testimonianze del/degli alunno/i, queste verranno raccolte e comunicate ai genitori e al Dirigente scolastico; per fatti criminosi anche alla polizia.
In particolare, la segnalazione viene fatta alle famiglie degli alunni coinvolti.
Per i reati più gravi il Dirigente Scolastico ha l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti).
In ogni situazione di sofferenza o disagio legato ad un uso scorretto del web e delle TIC
è possibile:

- riferire direttamente agli insegnanti o al team per la sicurezza online. Questi, dopo consultazione del Dirigente Scolastico, indirizzeranno l'alunno insieme alla famiglia verso i passi da compiere, rispetto alla gravità della situazione e se necessario metteranno in atto azioni di monitoraggio e accompagnamento;
- usufruire dello Sportello di Ascolto, se attivo, nel nostro Istituto. Esso è luogo di ascolto neutro e riservato. La/lo psicologa/o valuterà i singoli casi e come procedere. È invitata/o tuttavia a condividere con i referenti istituzionali nei limiti di rispetto del segreto professionale informazioni e azioni volte alla tutela e al benessere dei minori.

5.3 Gestione dei casi

La gestione dei casi rilevati andrà differenziata a seconda della loro gravità; è in ogni caso opportuna la condivisione a livello di Consiglio di Classe/Team di Docenti di ogni episodio rilevato.
Alcuni avvenimenti di lieve rilevanza possono essere affrontati e risolti con la discussione collettiva in classe.
Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e individuare una strategia comune per rimediare.

Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico come intervenire e segnalare alle autorità competenti.