DIREZIONE DIDATTICA 2° CIRCOLO

Via Santa Maria Mazzarello, s. n. - 93017 SAN CATALDO (CL)

www.circolo2sancataldo.edu.it. - clee02500p@istruzione.it

Tel. 0934/571394 - Fax 0934/571563 Cod. Fisc. 80005420858

Cod. Mecc. CLEE02500P

"Una scuola … per star bene"

Progetto Generazioni Connesse

DOCUMENTO DI

E-Safety Policy

A.S. 2019/2020

1.Introduzione

1.1. Scopo della Policy

La nostra istituzione scolastica ha elaborato questo documento con lo scopo di informare l'utenza per un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla scuola, e per gestire, prevenire situazioni problematiche.
In particolare il nostro intento è quello di promuovere l'uso adeguato e critico da parte degli alunni delle tecnologie digitali e di internet, di far acquisire loro, non solo competenze "tecniche," ma anche corrette norme comportamentali.
Gli utenti, adulti e minori, devono acquisire consapevolezza dei rischi a cui si espongono quando navigano in rete. Per questo motivo, gli insegnanti devono guidare gli studenti nelle attività online a scuola e indicare loro le regole di condotta per l'utilizzo sicuro di internet anche a casa.
La nostra Scuola, negli ultimi anni, ha incrementato molto l'uso delle tecnologie informatiche nella didattica e nell'organizzazione generale della scuola, non solo per svolgere esperienze formative, ma anche per condurre in modo più efficiente le funzioni amministrative.
Grazie all'implementazione del sito, all'introduzione del registro elettronico e all'utilizzo della piattaforma web Argo, a cui possono accedere Dirigente, docenti, genitori, alunni e personale amministrativo, è diventato più semplice gestire il sistema-scuola e aprire la scuola all'utenza con una comunicazione più tempestiva, chiara e trasparente.
Allo stesso tempo, l'uso di piattaforme web ha esposto gli utenti e in particolare i minori e i soggetti con limitate competenze informatiche a nuovi rischi. Per questo la nostra scuola ha deciso di partecipare al progetto "Generazioni Connesse" ed elaborare l'e-Safety Policy per:

- diffondere la conoscenza e comprensione da parte di tutto il personale scolastico delle procedure, monitoraggio e gestione di casi di abuso o di altre problematiche associate all'utilizzo di Internet e delle tecnologie digitali;
- disciplinare l'utilizzo delle TIC all'interno della scuola stessa (dotazione di filtri) e prevedere misure per prevenire diverse tipologie di rischio;
- promuovere la competenza digitale negli alunni e la cultura del rispetto di regole comuni nell'uso dei servizi telematici e lo sviluppo di regole di comportamento (Netiquette) riferite all'utilizzo dei Social Network.

1.2. Ruoli e responsabilità

1.2.1. Il Dirigente scolastico ha il compito di:

- garantire la sicurezza (tra cui la sicurezza on-line) dei membri della comunità scolastica;
- garantire a tutti gli insegnanti di ricevere una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze;
- 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.

1.2.2. L'Animatore digitale

Il ruolo dell'Animatore digitale include i seguenti compiti:

- 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;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola;
- individuare soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali;
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e a progetti attinenti la "scuola digitale";
- 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, affinché vengano adottate le procedure previste dalle norme.

1.2.3. Referente d'Istituto per il bullismo ed il cyberbullismo:

Ha il compito di coordinare le iniziative di prevenzione e di contrasto del Cyberbullismo, aiutando i docenti e i genitori, con la collaborazione delle Forze di Polizia (Legge n. 71 del 2017). Inoltre, ha il compito di supportare il Dirigente Scolastico nella revisione e stesura di Regolamenti d'Istituto, di atti e documenti.

1.2.4. Pronto soccorso tecnico

L'addetto al pronto soccorso tecnico ha i seguenti compiti:

- registra i disservizi e le problematiche relative alla rete e all'uso del digitale segnalate dai docenti e provvede, ove possibile, all'intervento tecnico.

1.2.5. Direttore dei servizi generali e amministrativi e docente su nomina del D.S.

Il ruolo del Direttore dei servizi generali e amministrativi si esplica attraverso le seguenti funzioni:

- assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;
- garantire il funzionamento dei diversi canali di comunicazione della scuola (circolari, sito web, ecc.) all'interno della stessa e fra la scuola e le famiglie degli alunni;
- controllare probabili azioni di cyber-bullismo.

1.2.6. Docenti

Il ruolo del personale docente prevede i seguenti compiti:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;

- garantire che gli alunni rispettino le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;
- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- nelle lezioni in cui è programmato l'utilizzo di internet, guidare gli alunni a siti controllati e comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare 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, affinché vengano applicate le procedure previste dalle norme.

1.2.7. Alunni

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;
- avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali, ma anche della necessità di evitare il plagio e di rispettare i diritti d'autore;
- comprendere l'importanza di adottare buone pratiche di sicurezza on-line 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.

1.2.8. Genitori

Il ruolo dei genitori degli alunni si svolge attraverso 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 gli alunni nello studio a casa, in particolare controllare l'utilizzo del pc e di internet;
- concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet;
- fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e del telefonino in generale.

1.3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto

Tutte le persone esterne che erogano attività educative nel nostro Istituto devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, ascoltare le opinioni ed i desideri dei minori. Sono vietati i comportamenti

irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli alunni. I soggetti esterni devono conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, PC, etc...) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli alunni. Inoltre devono rispettare la privacy degli alunni in quanto minori, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

1.4. Condivisione e comunicazione della Policy all'intera comunità scolastica.

1.4.1. Condividere e comunicare la politica di e-safety agli alunni

- Tutti gli alunni saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione.
- L'elenco delle regole per la sicurezza on-line sarà affisso in tutte le aule e nei laboratori con accesso a internet.

1.4.2. Condividere e comunicare la politica di e-safety al personale

- La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet sarà discussa negli Organi collegiali (Consigli di interclasse/intersezione, Collegio dei docenti) e comunicata formalmente a tutto il personale e pubblicata sul sito web.
- Il personale docente sarà reso consapevole del fatto che il traffico in internet può essere monitorato e si potrà risalire al singolo utente registrato.
- Un'adeguata informazione/formazione on-line del personale docente, nell'uso sicuro e responsabile di internet, sarà fornita dall'Animatore Digitale a tutto il personale, anche attraverso il sito web della scuola.
- Il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC sarà supervisionato dal responsabile, che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici.
- L'Animatore digitale metterà in evidenza on-line utili strumenti di informazione che il personale potrà usare con gli alunni in classe. Questi strumenti varieranno a seconda dell'età e della capacità degli alunni.
- Tutto il personale prenderà consapevolezza che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e con i propri doveri professionali è sanzionabile (Codice Disciplinare dei Dipendenti).

1.4.3. Condividere e comunicare la politica di e-safety ai genitori

- Sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione degli incontri scuola-famiglia.
- L'Animatore digitale fornirà ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di internet anche a casa.
- L'Animatore digitale e i docenti di classe forniranno ai genitori indirizzi web relativi a risorse utili per lo studio e a siti idonei ed educativi per gli alunni, sistemi di filtraggio e attività educative per il tempo libero.

1.5. Gestione delle infrazioni alla Policy

1.5.1. Disciplina degli alunni

Le infrazioni in cui è probabile che gli alunni possano incorrere a scuola nell'utilizzo della rete internet, in relazione alla fascia di età considerate, sono prevedibilmente le seguenti:

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

Sono previsti, da parte dei docenti, provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento, quali: il richiamo verbale, il richiamo scritto con annotazione sul diario, la convocazione dei genitori da parte degli insegnanti e da parte del Dirigente scolastico. Contestualmente sono previsti interventi di carattere educativo, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di promozione di rapporti amicali, della conoscenza e della gestione delle emozioni.

1.5.2. Disciplina del personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti possano incorrere nell'utilizzo delle tecnologie digitali e di internet possono essere le seguenti:

- un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connessi alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- una carente istruzione preventiva degli alunni sull'utilizzazione corretta e responsabile delle tecnologie digitali e di internet;
- una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- insufficienti interventi di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale di casi emersi.

1.5.3. Disciplina dei genitori

In considerazione dell'età degli alunni e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola.

Le situazioni familiari meno favorevoli sono:

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

- un utilizzo del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria indirizzi o contenuti non idonei.

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

1.6. Integrazione della Policy con Regolamenti esistenti

Il documento E-Policy è coerente con gli obiettivi dei documenti del PTOF e del PNSD, del Regolamento di Istituto, del Patto di Corresponsabilità, del RAV e del PdM.

1.7. Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

Il monitoraggio dell'implementazione della e-Policy e del suo eventuale aggiornamento sarà svolta ogni anno e sarà curato dal Dirigente scolastico con la collaborazione dell'Animatore digitale, del Team Digitale, del docente responsabile del Cyberbullismo e dei docenti delle classi, tramite questionari e conversazioni. Sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di internet. Il monitoraggio sarà rivolto anche agli insegnanti, al fine di valutare l'impatto della e-Policy e la necessità di eventuali miglioramenti.

2. Formazione e curricolo

La nostra scuola, in coerenza con quanto affermato nel PTOF 2019/2021 e ai sensi del PNSD (Piano Nazionale Scuola Digitale), attiva corsi di formazione per i docenti sull'uso delle TIC applicate alla didattica. Per il triennio 2019/2021 è stato elaborato, a cura dell'Animatore Digitale, il Piano triennale le cui azioni sono: formazione interna rivolta ai docenti, coinvolgimento della comunità scolastica, sviluppo di soluzioni innovative. Esso comprende corsi di formazione per sviluppare una serie di competenze digitali di base, che permettano agli alunni, di utilizzare in maniera consapevole e responsabile le più comuni tecnologie dell'informazione e della comunicazione. Competenze digitali trasversali a tutte le discipline finalizzate a far acquisire agli alunni la capacità di saper reperire, valutare, conservare, produrre documenti e semplici presentazioni, scambiare informazioni, comunicare e partecipare a piattaforme Social Network. Vengono attivati anche corsi di formazione per educare alla sicurezza online e all'uso della rete e incontri formativi con la Polizia Postale.

2.1. Curricolo sulle competenze digitali per gli alunni

Obiettivi e competenze:

1. Conoscere e utilizzare le nuove tecnologie per giocare, rappresentare e comunicare contenuti.
2. Sviluppare il pensiero computazionale attraverso il Coding.
3. Utilizzare un ambiente di programmazione visuale e i principali comandi di un programma per il Coding e la robotica.

4. Individuare le potenzialità, i limiti e i rischi nell'uso delle tecnologie.

Scuola dell'infanzia

- 1.a. Le parti del computer e le loro funzioni.
- 1.b. Uso di semplici software didattici.
- 2.a. Giochi di movimento su grandi scacchiere (Coding unplugged).
- 2.b. Utilizzo della piattaforma Code.org per l'esecuzione di attività Coding plugged.
- 3.a. Giochi di creatività e attività laboratoriali con metodologia Tinkering.

Scuola Primaria

1.a. Il computer e i suoi elementi (Hardware e software).
1.b. Le funzioni di base di un personal computer e di un sistema operativo: le icone, le finestre di dialogo, le cartelle, i file.
1.c. Utilizzo di programmi di grafica.
1.d. Uso di programmi di videoscrittura per la produzione di semplici testi.
1.f. Strumenti di presentazione e realizzazione di ipertesti con Power Point.
1.g. Uso dei software per creare editing video ed editing audio.
1.h. Uso dei software online per la creazione di eBook e di digital storytelling.
1.i. Utilizzo del foglio elettronico Excel.
1.l. Giochi didattici per ogni disciplina.
2.a. Coding unplugged (programmazione su carta a quadretti, algoritmi, Pixel Art...).
3.a. Coding plugged - Lezioni tecnologiche in Code.org.
3.b. Tinkering e creatività per costruire semplici oggetti.
3.c Utilizzo del software di programmazione Scratch.
4.a. Norme di sicurezza nell'utilizzo degli strumenti informatici.
4.b. Uso consapevole e corretto della rete internet.
4.c. Uso della rete Internet per ricercare dati, immagini e fare ricerche
4.d. Utilizzo di alcune funzioni di Google APPS.
4.e. Uso dei Social Network e dei nuovi strumenti di comunicazione e condivisione delle informazioni.
4.f. Uso critico dei motori di ricerca: vantaggi e rischi.
4.g. Regole per navigare in modo sicuro e responsabile in rete ed essere consapevoli delle conseguenze di comportamenti inadeguati.
4.h. Conoscere e rispettare le norme relative ai copyright.
4.i. Conoscere i fenomeni del cyberbullismo, grooming…
4.l. Saper individuare e segnalare agli adulti di riferimento comportamenti inadeguati osservati in rete.
4.m. Essere consapevoli dei rischi connessi alla pubblicazione on-line di foto, video e dati personali propri e di altri (chat, social network...).

2.2. Formazione dei Docenti sull'integrazione delle TIC nella didattica

Quest'anno, per realizzare le azioni relative al PNSD, è stato elaborato, a cura dell'Animatore Digitale, il progetto per la formazione interna dei docenti per far conoscere software e APP ed acquisire competenze digitali sull'utilizzo e l'integrazione delle TIC nella didattica, per creare contenuti digitali. Nello stesso progetto sono stati previsti anche corsi di formazione sulla Didattica a distanza.
La scuola ha aderito anche ai corsi di formazione della rete territoriale.

Per i successivi anni scolastici, relativi al suddetto triennio, si terranno in considerazione i bisogni formativi dei docenti e si attiveranno corsi di formazione relativi alle tematiche maggiormente richieste. La progettazione degli interventi formativi ha come punto di partenza l'individuazione di competenze digitali che ogni docente oggi dovrebbe avere.

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

Il nostro PNSD prevede anche la formazione dei docenti su:

- Sicurezza in rete e sulla conoscenza dei rischi di un uso improprio delle TIC e della rete.
- Partecipazione al progetto "Generazioni Connesse"
- Partecipazione all'Evento Nazionale "Safer Internet Day"
- Uso dei Social Network ai fini didattici.
- Iscrizione alla Piattaforma ELISA (formazione e-learning sul bullismo e Cyberbullismo).
- Condivisione della documentazione fornita, durante la formazione e-learning sul bullismo e Cyberbullismo, a tutti i docenti.

2.4. Sensibilizzazione delle famiglie

Si avrà cura di sensibilizzare i genitori alla tematica della sicurezza in rete per accompagnarli verso un uso più responsabile e consapevole e informarli sulle situazioni di rischio on-line e sulle misure di restrizione da attivare per far utilizzare in sicurezza la rete ai minori.
A tal fine si sensibilizzeranno i genitori a consultare il portale "www.generazioniconnesse.it", si presenterà l'E-Safety Policy ai genitori nei Consigli di classe e di Interclasse, e si pubblicherà nel sito web della scuola. Si faranno, inoltre, degli incontri formativi con la Polizia Postale per i genitori, alunni e docenti.

3. Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella della scuola.

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

La scuola dispone di una rete LAN per gli uffici amministrativi e di una rete per la didattica. Il collegamento di computer portatili o Tablet personali alla rete di Istituto deve essere autorizzato dal Dirigente Scolastico.
Si connette a Internet tramite ADSL attraverso la rete LAN e rete Wi-fi collegati a un server PROXY. L'accesso a internet è possibile sia in classe che nei laboratori multimediali. L'accesso è per tutti schermato da filtri che impediscono il collegamento a siti appartenenti alla black list e che consentono, invece, il collegamento solo a siti sicuri e idonei alla didattica, secondo le impostazioni date dal responsabile tecnico che periodicamente provvede alla manutenzione e all'aggiornamento del sistema informatico del laboratorio, ove è necessario si richiede l'intervento di tecnici esterni. Tutti i PC sono forniti di antivirus.
L'accesso ai PC dei laboratori multimediali e ai PC delle aule, è consentito al personale docente attraverso l'assegnazione di una password da parte del Responsabile dell'area tecnologica di Istituto che coincide con la F.S. Area 2 "Sostegno al lavoro dei docenti - Coordinamento e gestione delle tecnologie informatiche e della comunicazione".

I docenti che accedono ai laboratori multimediali, registrano il proprio accesso, scrivendo su un registro la data e l'orario di utilizzo del laboratorio. In ogni laboratorio multimediale c'è un server che è la postazione di lavoro per il docente e i PC per gli alunni. Le postazioni degli alunni possono essere utilizzate anche dai docenti, i quali possono accedere tramite password.
Dal server il docente può controllare le postazioni degli alunni tramite il software della rete didattica. I file elaborati devono essere salvati, dai docenti interessati, sui supporti rimovibili personali, in quanto le postazioni del laboratorio funzionano come stazioni di lavoro e non come archivi.
Tutti i dispositivi in uso nella scuola sono muniti di antivirus. Il responsabile del laboratorio informatico, che attualmente coincide con la figura della F.S. Area 2 "Sostegno al lavoro dei docenti - Coordinamento e gestione delle tecnologie informatiche e della comunicazione", periodicamente provvede alla manutenzione del laboratorio informatico richiedendo, ove necessario, anche l'intervento di tecnici esterni.

3.2. Gestione accessi (password, backup, etc...)

La rete possiede un sistema di navigazione che viene gestita da un server proxy che controlla la navigazione degli accessi di tutti i PC collegati. Ad ogni PC si accede tramite password che vengono aggiornate periodicamente. Le postazioni degli alunni hanno due account, uno per il docente, il quale accede tramite password, e uno per gli alunni. Il PC collegato alla LIM, di ogni aula, viene utilizzato solo dal docente, il quale accede tramite password comune. Ogni docente ha una password personale per accedere al registro ARGO Nuovo Didup. Le operazioni di configurazione e di ripristino dei PC dei laboratori e delle classi viene fatto dal Responsabile dell'Area Tecnologica e dal tecnico esterno. Le operazioni di backup vengono effettuati solo nei PC degli uffici di segreteria.
È possibile effettuare installazioni e aggiornamenti di software solo tramite la password di amministratore, fornita al responsabile dell'area tecnologica (Animatore Digitale).

3.3. E-mail

L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. L'eventuale invio o ricevimento di posta a scopi didattici avverrebbe solo su autorizzazione del Dirigente scolastico e operativamente sarebbe svolto dall'Assistente Amministrativo addetto. La posta elettronica è protetta da antivirus, e quella certificata anche dall'antispam. Tutti i docenti possiedono una mail professionale e una privata.

3.4. Sito web della scuola e Blog

Il sito della scuola **www.circolo2sancataldo.edu.it** viene gestito dall'Animatore Digitale (F.S. Area 2 "Coordinamento e gestione delle tecnologie informatiche e della comunicazione), per l'inserimento dei contenuti e viene monitorato costantemente. I dati di tipo economico-amministrativo vengono inseriti dagli addetti del personale di Segreteria; l'inserimento dei contenuti vengono pubblicati, sotto la supervisione del Dirigente che ne valuta la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto

della privacy, secondo il regolamento del "**Codice in materia della protezione dei dati personali"**. Nel sito è stato inserito il collegamento al portale ARGO, alla quale possono accedere sia i docenti che i genitori grazie a password dedicate e personali.
L'Istituto attualmente ha anche un Blog, dal titolo "**Security in rete**", che intende offrire all'utenza un percorso guidato sulle tematiche della sicurezza on line e all'uso delle tecnologie nella didattica, delle misure da adottare per educare gli alunni al loro utilizzo e ad una fruizione responsabile della rete.

3.5. Social network

Attualmente nella didattica si utilizza la piattaforma Social Learning Edmodo. L'istituzione scolastica ha creato una pagina Facebook con il proprio profilo che viene gestita dall'Animatore Digitale sotto la supervisione del Dirigente.

3.6. Protezione dei dati personali

Il personale scolastico e amministrativo sono "incaricati del trattamento" dei dati personali nel rispetto delle norme previste in materia per fini burocratici e organizzativi.
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.
Viene inoltre richiesta l'autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori.
Ogni docente è responsabile delle proprie credenziali di accesso al registro elettronico ed è stato raccomandato di non salvare mai le proprie password, di effettuare il logout dalle proprie caselle di posta elettronica, di utilizzare password sicure e cambiarle ogni tre mesi.

4. Strumentazione personale

4.1. Per gli studenti: gestione degli strumenti personali

Non è consentito l'utilizzo di strumentazioni elettroniche personali, tranne se richiesto dai docenti per attività didattiche finalizzate ad attuare il BYOD a scuola.

4.2. Per i docenti: gestione degli strumenti personali

Durante le ore delle lezioni non è consentito l'utilizzo del cellulare, mentre è possibile fruire di altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili.
I docenti possono utilizzare dispositivi in dotazione della scuola esclusivamente per fini didattici.
L'uso incauto dei dispositivi comuni può essere addebitato al responsabile del danno attraverso la tracciabilità dell'accesso.
L' utilizzo dei dispositivi in uso e della rete WI-FI sarà autorizzato, previa richiesta e rilascio di credenziali di accesso, dal D.S. che ne valuterà la coerenza con gli scopi didattici garantiti dal richiedente.
Il collegamento di qualsiasi dispositivo potrà essere monitorato e controllato attraverso software di gestione della rete.

Se a scuola vengono utilizzati dispositivi di archiviazione esterna di proprietà personale (chiavette usb, hard disk portatili) è opportuno controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.

4.3. Per il personale della scuola: gestione degli strumenti personali

Durante l'orario di servizio al restante personale scolastico è consentito l'utilizzo dei propri devices (cellulare) solo per comunicazioni personali di carattere urgente, e solo a condizione che non impedisca il normale svolgimento dei propri compiti.

5. Rischi on line: conoscere, prevenire e rilevare

5.1. Sensibilizzazione e prevenzione

I rischi effettivi che gli alunni possono incontrare a scuola derivano dall'utilizzo dei PC del laboratorio informatico. Infatti, può accadere che, eludendo la vigilanza degli insegnanti, gli alunni si colleghino e scaricano foto personali o di altri, immagini e video con contenuti violenti e non adatti alla loro età, a siti poco sicuri per scaricare immagini e foto con sfondo sessuale, o si colleghino a videogiochi diseducativi con il rischio di essere contattati da adulti con intenzioni malevoli, o per comunicare e chattare con sconosciuti con il rischio di adescamento online (grooming), o per inviare e/o ricevere messaggi di molestia e minacce da coetanei (cyberbullismo).
Per evitare questo è necessario e indispensabile che gli alunni acquisiscano quelle competenze e capacità adeguate per utilizzare in modo consapevole le Nuove Tecnologie.
I docenti pertanto hanno il compito di attivare percorsi formativi di prevenzione e formare gli alunni sulla sicurezza online e promuovere le competenze digitali per evitare i rischi legati all'uso del digitale.
In questo percorso formativo, la scuola può avvalersi della collaborazione delle ASL e della Polizia Postale.
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.
- Fornire ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori (es. liberatoria per la pubblicazione delle eventuali foto, immagini, testi e disegni relativi al proprio/a figlio/a).
- Non consentire l'utilizzo del cellulare personale degli alunni a scuola, in quanto per assolvere a ogni comunicazione urgente con i genitori o con chi ne fa le veci è sempre disponibile il telefono della scuola.
- Utilizzare filtri e software che impediscono il collegamento ai siti web per adulti (black list).

LINEE GUIDA PER ALUNNI

- Non comunicare mai a nessuno la tua password e periodicamente va cambiata, usando numeri, lettere e caratteri speciali.

- Mantieni segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della tua

scuola.

- Non inviare a nessuno fotografie tue o di tuoi amici; prima di inviare o pubblicare su un BLOG la fotografia di qualcuno, chiedi sempre il permesso.

- Chiedi sempre al tuo insegnante o ai tuoi genitori il permesso di scaricare documenti Internet.

- Chiedi sempre il permesso prima di iscriverti a qualche concorso o prima di riferire l'indirizzo della tua scuola.

- Quando sei connesso alla rete RISPETTA SEMPRE GLI ALTRI, ciò che per te è un gioco può rivelarsi offensivo per qualcun altro.

- Non rispondere alle offese e agli insulti.

- Blocca i Bulli: molti Blog e siti social network ti permettono di segnalare i cyberbulli.

- Conserva le comunicazioni offensive, ti potrebbero essere utili per dimostrare quanto ti è accaduto.

- Se ricevi materiale offensivo (e-mail, sms, video, foto, messaggi vocali) non diffonderlo: potresti essere accusato di cyberbullismo.

- Rifletti prima di inviare: ricordati che tutto ciò che invii su internet diviene pubblico e rimane per SEMPRE.

- Riferisci al tuo insegnante o ai tuoi genitori se qualcuno ti invia immagini che ti infastidiscono e non rispondere; riferisci anche al tuo insegnante o ai tuoi genitori se ti capita di trovare immagini di questo tipo su Internet.

- Se qualcuno su Internet ti chiede un incontro di persona, riferiscilo al tuo insegnante o ai tuoi genitori.

- Ricordati che le persone che incontri nella Rete sono degli estranei e non sempre sono quello che dicono di essere.

- Non è consigliabile inviare e-mail personali, perciò rivolgiti sempre al tuo insegnante prima di inviare messaggi di classe o ai tuoi genitori prima di inviare messaggi da casa.

- Non scaricare (download) o copiare materiale da Internet senza il permesso del tuo insegnante o dei tuoi genitori;

- Non caricare (upload) materiale video o fotografico nei siti web dedicati senza il permesso del tuo insegnante o dei tuoi genitori.

LINEE GUIDA PER INSEGNANTI

- Evitate di lasciare le e-mail o file personali sui computer o sul server della scuola, lo spazio è limitato e di uso comune.

- Salvate sempre i vostri lavori (file) in cartelle personali e/o di classe e non sul desktop o nella cartella del programma in uso. Sarà cura di chi mantiene il corretto funzionamento delle macchine cancellare file di lavoro sparsi per la macchina e al di fuori delle cartelle personali;

- Discutete con gli alunni della policy e-safety della scuola, dell'utilizzo consentito della rete, e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di Internet.

- Date chiare indicazioni agli alunni su come si utilizza Internet, ed eventualmente anche la posta elettronica, e informateli che le navigazioni saranno monitorate.

- Ricordate di disconnettervi dal proprio account, di uscire da tutte le sessioni di lavoro su Internet e di spegnere il computer.

- Ricordate agli alunni che la violazione consapevole della Policy e-safety della scuola comporta sanzioni di diverso tipo.

- Adottate provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento.

- Adottate interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe.

- Nelle situazioni psico-socio-educative particolarmente problematiche, convocate i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi.

- Chiedete/suggerite di cancellare il materiale offensivo, bloccare o ignorare particolari mittenti.

- Segnalate la presenza di materiale pedopornografico (senza scaricarlo o riprodurlo) alla Polizia Postale o al Telefono Azzurro.

- In caso di abuso sessuale rilevato anche attraverso i nuovi mezzi di comunicazione, come internet o il cellulare, confrontatevi con i colleghi di classe e il Dirigente Scolastico, denunciate all'autorità giudiziaria o agli organi di Polizia.

CONSIGLI AI GENITORI PER UN USO RESPONSABILE DI INTERNET A CASA

- Posizionate il computer in salone o in una stanza accessibile a tutta la famiglia.

- Evitate di lasciare le e-mail o file personali sui computer di uso comune.

- Concordate con vostro figlio le regole: quando si può usare internet e per quanto tempo...

- Inserite nel computer i filtri di protezione: prevenite lo spam, i pop-up pubblicitari, l'accesso a siti pornografici.

- Aumentate il filtro del “parental control” attraverso la sezione sicurezza in internet dal pannello di controllo; attivate il firewall (protezione contro malware) e antivirus.

- Mostratevi coinvolti: chiedete a vostro figlio di mostrarvi come funziona internet e come viene usato per scaricare e caricare compiti, lezioni, materiali didattici e per comunicare con l'insegnante.

- Incoraggiate le attività on-line di alta qualità: ricercare informazioni scientifiche, ricercare nuovi amici nel mondo.

- Partecipate alle esperienze on-line: navigate insieme a vostro figlio, incontrate amici on-line, discutete degli eventuali problemi che si presentano.

- Spiegate a vostro figlio che la password per accedere ad alcune piattaforme è strettamente personale e non deve essere mai fornita ai compagni o ad altre persone.

- Stabilite ciò che ritenete inaccettabile (razzismo, violenza, linguaggio volgare, pornografia).

- Discutete sul tema dello scaricare file e della possibilità di ricevere file con virus da siti sconosciuti.

- Incoraggiate vostro figlio a dirvi se vedono immagini particolari o se ricevono e-mail indesiderate.

- Discutete nei dettagli le conseguenze che potranno esserci se vostro figlio visita deliberatamente siti non adatti, ma non rimproveratelo se compie azioni involontarie.

- Il modo migliore per proteggere vostro figlio è usare Internet con loro, discutere e riconoscere insieme i rischi potenziali.

6. Segnalazione e gestione dei casi

6.1. Cosa segnalare

- I contenuti “pericolosi” comunicati/ricevuti da altri, messi e/o scaricati in rete, ovvero le tracce che possono comprovare l’utilizzo incauto o scorretto degli strumenti digitali.
- Contenuti afferenti alla privacy (foto personali, l'indirizzo di casa o il telefono, password, 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, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc...).

6.2. Come segnalare: quali strumenti e a chi

L’insegnante che nota dei comportamenti anomali tra gli alunni della propria classe riconducibili a un disagio riferibile a un episodio di bullismo e/o cyberbullismo, può utilizzare i seguenti strumenti:

- Diario di Bordo o schema riepilogativo per la segnalazione dei rischi online (Allegato A).
- Sondaggio da somministrare agli alunni per rilevare episodi di bullismo tra gli alunni (Allegato B).
- Il modulo per la segnalazione dei casi (Allegato C).

Se questi episodi vengono ripetuti nel tempo allora il docente deve coinvolgere il referente d'Istituto per il contrasto del bullismo e del cyberbullismo, avvisare il Consiglio di classe e il Dirigente Scolastico.
Il Dirigente Scolastico, dopo la segnalazione, avrà cura di contattare il docente, per un confronto, al fine di valutare gli interventi educativi e coinvolgerà i genitori e anche la psicopedagogista della scuola per attivare e programmare insieme un percorso condiviso a sostegno del disagio.
A seconda della situazione e delle valutazioni effettuate con il referente, la psicopedagogista, il dirigente e i genitori, se c'è un reato grave di cyberbullismo, sulla base della legge del 29 maggio, 71/2017, si dovrà contattare la Polizia Postale per sporgere regolare denuncia.
La segnalazione deve essere supportata da prove specifiche e/o testimonianze. Pertanto è necessario che il docente conservi le prove della condotta incauta, scorretta o dell'abuso rilevate sui PC della scuola: soprattutto la data e l'ora, il contenuto dei messaggi o l'indirizzo web del profilo ed il suo contenuto. Per gli eventuali collegamenti non autorizzati a siti, social network, video-hosting sites e altri website, l'insegnante può conservare il link, stampare la pagina o salvare la schermata su documento word. Per l'e-mail si può stampare la stessa o conservare l'intero messaggio, compresa l'intestazione del mittente.
Conservare la prova è utile per far conoscere l'accaduto, in base alla gravità, ai genitori degli alunni, al Dirigente Scolastico e alla polizia.
Per le segnalazioni di fatti rilevati sono previsti i seguenti strumenti, in base alla gravità del caso:

- Annotare il comportamento sul registro.
- Avvisare il referente del bullismo e del cyberbullismo.
- Informare il Dirigente scolastico.
- Richiedere la consulenza dello psicologo e/o della psicopedagogista della scuola.
- Comunicare, per iscritto o attraverso un colloquio, l'accaduto ai genitori (o con chi esercita la responsabilità genitoriale) degli alunni.
- Convocare il Consiglio di Classe.
- A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnalare alla Polizia Postale.

In base all'urgenza, le comunicazioni formali possono essere precedute da quelle informali, effettuate per le vie brevi. Inoltre per i reati meno gravi la legge rimette ai genitori degli alunni la scelta di richiedere la punizione del colpevole, attraverso la querela. Per i reati più gravi (es. pedopornografia) gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti).

6.3. Come gestire le segnalazioni a seconda dei casi

Accorgersi, dunque, tempestivamente, di quanto accade e compiere azioni immediate di contrasto verso comportamenti e atti ritenuti pericolosi, diviene fondamentale per evitare conseguenze che possano compromettere il benessere psicologico e la crescita armonica dei soggetti coinvolti. Il compito dei docenti non è solo quello di segnalare, ma è soprattutto

quello di prevenire i casi di bullismo attraverso interventi educativi e attività finalizzate al rispetto delle regole della convivenza civile e democratica. La gestione dei casi evidenziati va differenziata a seconda della loro gravità e condivisa collegialmente dai docenti per valutare insieme le azioni da intraprendere per:

- dare sostegno alla vittima;
- lavorare sul gruppo classe affinché riconosca la gravità dell'accaduto e la propria partecipazione attraverso il silenzio o forme blande di coinvolgimento;
- dare supporto al bullo con un programma educativo che si focalizzi su due fronti: il coinvolgimento attivo del gruppo dei pari per sviluppare l'empatia e l'intervento dei docenti per gestire l'aggressività e la rabbia e nei casi più difficili richiedere la consulenza di uno specialista.

Come già detto per la prevenzione, il coinvolgimento dei coetanei è indispensabile per garantire l'efficacia dell'intervento ed è finalizzato a:

- creare un clima di solidarietà;
- combattere l'indifferenza e la deresponsabilizzazione morale;
- incoraggiare le vittime a chiedere aiuto.

Gestione delle segnalazioni a seconda dei casi

CASI	GESTIONE
Casi di "immaturità": Potrebbe accadere all'alunno di fornire i propri dati sui siti che attraggono l'attenzione dei bambini, con giochi e animazioni e che richiedono una procedura di registrazione.	I comportamenti devono essere controllati e contenuti dai docenti attraverso i normali interventi educativi.
Casi di "prepotenza" o "prevaricazione": I comportamenti di prepotenza possono esprimersi nelle forme più varie. Le caratteristiche che aiutano a individuarli e a distinguerli dallo scherzo sono la costanza nel tempo e la ripetitività. Per interpretare meglio questi segnali è opportuno tenere presenti alcuni indicatori che ci possono aiutare per verificare se nella classe sono presenti episodi di prevaricazione. Per arrivare all'identificazione del problema può essere di aiuto il materiale di supporto dell'area scuole del sito generazioni connesse.	Per prevenire e affrontare il bullismo i docenti devono attivare percorsi sia per le vittime che per i prepotenti e intervenire coinvolgendo i genitori degli alunni. Devono essere intrapresi anche percorsi individualizzati di sostegno alle vittime, volti a incrementarne l'autostima e l'assertività e a potenziare le risorse di interazione sociale, mentre i prevaricatori sono destinatari di interventi mirati a favorire una loro condivisione delle norme morali. Inoltre la scuola, qualora rilevi una situazione particolarmente problematica, deve convocare i genitori o gli esercenti la potestà per valutare gli interventi educativi da attivare con loro a quali risorse territoriali possono rivolgersi.

Casi di Cyberbullismo: Nel caso particolare del Cyberbullismo, le molestie sono messe in atto attraverso l'uso di Internet e delle tecnologie digitali: -diffusione di messaggi offensivi ai danni della vittima, attraverso la divulgazione di sms, messaggi in chat, e-mail offensive o di minaccia -pubblicazione di foto e filmati che ritraggono prepotenze o in cui la vittima viene offesa.	Gli interventi rivolti al gruppo classe sono gestiti in collaborazione dal Consiglio di classe e dalle famiglie, con percorsi didattici specifici volti alla gestione positiva del conflitto (gruppi di discussione, attività di role-play sull'argomento, strategie del problem solving, ecc...) In situazioni particolarmente problematiche, la scuola convoca i genitori per valutare con loro a quali risorse territoriali possono rivolgersi. Consiglia di servirsi: - dello sportello di ascolto psicologico attivo presso la scuola. -dei Servizi Sociali dell'Ente Locale per la fruizione di servizi socio-educativi comunali -dell' ASL per la competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Psicologo).
Casi di abuso sessuale e di adescamento online Nel caso in cui l'alunno: -scarica immagini e video pornografici e li diffonde, o produce video che sfuggano al suo controllo e vengano diffuse senza il suo consenso; - è indotto a spogliarsi e viene ripreso con il cellulare oppure è indotto a inviare una foto che lo ritrae nudo in Internet; - subisce ricatti ed è costretto a non rivelare gli abusi.	E' opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere, per quanto possibile, la rimozione del materiale (se online) e il blocco della sua diffusione via dispositivi mobili. E' opportuno fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto. È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Ascoltare la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, in sede di raccolta di informazioni, con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

6.4. Allegati con le procedure

6.4.1. Procedure operative per la gestione delle infrazioni alla Policy

- Segnalare all'Animatore Digitale

- L’Animatore valuterà se intervenire personalmente (nei casi più lievi) oppure se riferire al Dirigente (nei casi più gravi).
- Le procedure, da applicarsi secondo i criteri dettati dalla e-policy, sono incluse nel Codice Disciplinare, nel Patto di corresponsabilità e nel PTOF.

6.4.2. Procedure operative per la protezione dei dati personali (per docenti)

- Creare password sicure e cambiarle ogni tre mesi.
- Non comunicare mai le proprie password.
- Nella navigazione on-line, assicurarsi di negare sempre il consenso ad ogni richiesta di salvare le password utilizzate.
- Utilizzare gli applicativi CLOUD (Dropbox, Google Drive, One Drive), per lavorare sui PC comuni della scuola, evitando così di salvare nella memoria interna del PC.
- Prima di lasciare una postazione comune, assicurarsi di aver cancellato ogni file scaricato o elaborato, di uscire dall’applicativo utilizzato e di spegnere il PC.
- Tutti i dati personali degli alunni devono essere trattati in modo lecito e corretto.
- E’ obbligatorio chiedere il permesso ai genitori prima di pubblicare foto e video dei loro figli.

6.4.3. Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni e dei casi

In merito alle procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni e dei casi, si rinvia a quanto già affermato in altro paragrafo del presente documento.

6.4.4. Protocolli siglati con le forze dell’ordine e i servizi del territorio per la gestione condivisa dei casi.

Esistono prassi informali, costruite nel tempo, con le autorità competenti e con i servizi socio-sanitari del territorio per la gestione condivisa dei casi.

ALLEGATI

1. **ALLEGATO A (DIARIO DI BORDO - SCHEMA RIEPILOGATIVO PER LA SEGNALAZIONE DEI RISCHI ONLINE)**
2. **ALLEGATO B (SONDAGGIO PER LA RILEVAZIONE DEI CASI DI BULLISMO)**

3. ALLEGATO C (MODULO PER LA SEGNALAZIONE DI CASI)

DIREZIONE DIDATTICA 2° CIRCOLO

Via Santa Maria Mazzarello, s. n. - 93017 SAN CATALDO (CL)
www.circolo2sancataldo.edu.it. - clee02500p@istruzione.it
Tel. 0934/571394 - Fax 0934/571563 Cod. Fisc. 80005420858 – Cod. Mecc. CLEE02500P
Una scuola ... per star bene

ALLEGATO A
Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi
Scuola _____ Anno Scolastico _____

N°	Data	ora	Episodio *(riassunto)*	Azioni intraprese		Insegnante con cui l'alunno/a si è confidato	Firma
				Cosa?	Da chi?		

DIREZIONE DIDATTICA 2° CIRCOLO

Via Santa Maria Mazzarello, s. n. - 93017 SAN CATALDO (CL)
www.circolo2sancataldo.edu.it. - clee02500p@istruzione.it
Tel. 0934/571394 - Fax 0934/571563 Cod. Fisc. 80005420858 – Cod. Mecc. CLEE02500P
Una scuola ... per star bene

ALLEGATO B
Sondaggio per rilevare i casi di Bullismo

1. I tuoi amici di scuola ti hanno mai escluso?
   - o Mai
   - o Qualche volta
   - o Spesso
   - o Sempre

2. Sei stato mai maltrattato o spinto?
   - o Mai
   - o Qualche volta
   - o Spesso
   - o Sempre

3. Sei stato mai preso in giro?
   - o Mai
   - o Qualche volta
   - o Spesso
   - o Sempre

4. Ne hai parlato con qualcuno?
- Con un amico
- Con i genitori
- Con l'insegnante
- Con fratello/sorella
- Con nessuno

5. Se non ne hai parlato con nessuno, perché?

- Nessuno mi può aiutare
- Mi vergogno un po'
- Spero finisca presto

6. Qualche tuo compagno viene preso in giro?

- Mai
- Qualche volta
- Spesso
- Sempre

7. In quali luoghi?

- Fuori dalla scuola
- Durante la ricreazione
- In aula
- In bagno
- Nei corridoi

8. Hai subito offese, molestie o minacce da parte di qualcuno attraverso internet, cellulare o altro mezzo digitale? (fuori dalla scuola)

- non è mai successo
- è successo una o due volte
- è successo poche volte
- è successo diverse volte
- è successo spesso

9. Cosa ti è successo? (è possibile dare più di una risposta)

- mi hanno inviato dei messaggi volgari, offensivi o minacciosi
- hanno scritto di me cose non vere, e false per danneggiarmi
- hanno postato, pubblicato, fotografie o video imbarazzanti/umilianti che mi ritraevano
- mi hanno escluso per dispetto da un gruppo on-line (chat, social, community)
- qualcuno ha creato un falso profilo su di me, su una chat o un social network.

ALLEGATO C - MODULO PER LA SEGNALAZIONE DEI CASI

Generazioni Connesse

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

Co-financed by the European Union
Connecting Europe Facility

MODULO PER LA SEGNALAZIONE DI CASI

Nome di chi compila la segnalazione:	Ruolo:
Data:	Scuola:

Descrizione dell'episodio o del problema		
Soggetti coinvolti	Vittima/e: 1..... Classe: .... 2..... Classe: .... 3..... Classe:	Autore/autrice e sostenitori: 1..... Classe: .... 2..... Classe: .... 3..... Classe: ....
Chi ha riferito dell'episodio?	- La vittima - Un compagno della vittima, nome: - Genitore, nome: - Insegnante, nome: - Altri, specificare:	
Atteggiamento del gruppo	Da quanti compagni è sostenuto il bullo? Quanti compagni supportano la vittima o potrebbero farlo?	
Gli insegnanti sono intervenuti in qualche modo ?		
La famiglia o altri adulti hanno cercato di intervenire ?		
Chi è stato informato della situazione?	□ coordinatore di classe data: □ consiglio di classe data: □ dirigente scolastico data: □ la famiglia della vittima/e data:	□ la famiglia del bullo/i data: □ le forze dell'ordine data: □ altro, specificare:

San Cataldo li, 22/06/2020

IL DIRIGENTE SCOLASTICO

Dott.ssa Calogera Duminuco

Firmato digitalmente da **CALOGERA DUMINUCO**