Unione Europea * Ministero Istruzione Università Ricerca * Regione Sicilia * Distretto Scolastico n. 1

Istituto di Istruzione Secondaria Superiore Statale

"Don Michele Arena"

Via V. Nenni, 2 - ☎0925/22510 - Fax 0925/24247 == Via Giotto, 20 - ☎0925/85365 - Fax 0925/85366
Corso A. Miraglia, 13 - ☎0925/22239 - Fax 0925/23410 == Via Eta, 12 (92016 Menfi) - ☎ / Fax 0925/74214
E-Mail: agis01600n@istruzione.it – agis01600n@pec.istruzione.it - URL: www.iissarena.gov.it - C.F. 92002960844
92019 SCIACCA (AG)

E-Safety Policy

Misure atte a facilitare e promuovere l'utilizzo positivo delle TIC nella didattica e negli ambienti scolastici; misure di prevenzione e misure di gestione di situazioni problematiche relative all'uso delle tecnologie digitali.

Approvato dal Collegio dei Docenti con delibera n. 23 del giorno 24/10/2018.
Adottato dal Consiglio di Istituto con delibera n. 24 del giorno 29/10/2018.

INDICE RAGIONATO

1. **Introduzione**
   - 1.1. Scopo della Policy.
   - 1.2. Ruoli e Responsabilità (che cosa ci si aspetta da tutti gli attori della Comunità Scolastica).
   - 1.3. Condivisione e comunicazione della Policy all'intera comunità scolastica.
   - 1.4. Gestione delle infrazioni alla Policy.
   - 1.5. Monitoraggio dell'implementazione della Policy e suo aggiornamento.
   - 1.6. Integrazione della Policy con Regolamenti esistenti.
2. **Formazione e Curricolo**
   - 2.1 Curricolo sulle competenze digitali per gli studenti.
   - 2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica.
   - 2.3 Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
   - 2.4 Sensibilizzazione delle famiglie.
3. **Gestione dell'infrastruttura e della strumentazione ICT della scuola**
   - 3.1 Accesso ad internet: filtri antivirus e sulla navigazione.
   - 3.2 Gestione accessi (password, backup, ecc.).
   - 3.3 E-mail.
   - 3.4 Blog e sito web della scuola
   - 3.5 Social network.
   - 3.6 Protezione dei dati personali.
4. **Strumentazione personale**
   - 4.1 Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc..
   - 4.2 Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc..
   - 4.3 Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc..
5. **Prevenzione, rilevazione e gestione dei casi**

   Prevenzione
   - Rischi
   - Azioni

   Rilevazione
   - Che cosa segnalare
   - Come segnalare: quali strumenti e a chi.
   - Come gestire le segnalazioni.

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

Annessi

1. Procedure operative per la gestione dei casi
2. Procedure operative per la gestione delle infrazioni alla Policy.
3. Procedure operative per la protezione dei dati personali.

1. INTRODUZIONE

1.1. Scopo della Policy

La Policy è un documento/guida che raccoglie le norme comportamentali da seguire per promuovere un utilizzo consapevole e corretto della rete e, più in generale, delle Tic all'interno del contesto scolastico. Viene applicata a tutti i membri della comunità scolastica che hanno accesso o che sono utenti dei sistemi informatici dell' Istituto in quanto la presenza sempre più diffusa delle tecnologie digitali offre grandi possibilità di trasformazione del processo di insegnamento/apprendimento, ci impone una riflessione sul loro uso efficace, sicuro e consapevole e ci mette di fronte a sfide importanti, che riguardano più livelli di conoscenze, abilità e attitudini che i più giovani hanno bisogno di sviluppare, accrescere e correggere. La scuola, quindi, ha il compito di prevenire, rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso delle tecnologie digitali al fine di evitare l'occorrenza di atti che non solo creino disagio nella comunità scolastica, ma che possono configurarsi come reati. La Policy è uno strumento in divenire, va monitorata e implementata annualmente, se necessario, contestualmente al Rapporto di Autovalutazione, sulla base di questionari, di eventuali situazioni problematiche affrontate o di esigenze e sollecitazioni che emergono dalle diverse componenti dell'Istituto.

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

Nell'ambito di questa policy sono individuati i seguenti ruoli e le principali responsabilità correlate:

RUOLI	RESPONSABILITA'
1) **DIRIGENTE SCOLASTICO**	▪ ha la responsabilità generale per i dati e la loro sicurezza; ▪ cura la sicurezza on-line della comunità scolastica; ▪ garantisce la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i menbri della comunità scolastica; ▪ ha la responsabilità di assicurare che il personale riceva una formazione adeguata per svolgere i ruoli di sicurezza on-line e per la formazione di altri colleghi; ▪ garantisce che vi sia un sistema in grado di monitorare il personale di supporto che svolge le procedure di sicurezza online interne.
2) **IL DSGA**	▪ assicura, 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; ▪ garantisce che sia tenuto un registro di incidenti di sicurezza online; ▪ coordina con le autorità locali e le agenzie competenti; ▪ controlla l'accesso a materiali illegali/inadeguati; ▪ controlla eventuali azioni di cyberbullismo.
3) **ANIMATORE DIGITALE E TEAM DELL'INNOVAZIONE**	▪ promuovono l'aggiornamento dei docenti; ▪ contribuiscono alla diffusione dell'innovazione nella scuola, a partire dai contenuti del Pnsd; ▪ sviluppano progettualità sugli ambiti della formazione interna e sulla creazione di soluzioni innovative.
4) **DOCENTE FUNZIONE STRUMENTALE PER LE NUOVE TECNOLOGIE**	▪ cura il sito web della scuola per scopi istituzionali e consentiti; ▪ supporta l'attività laboratoriale con consigli, aiuti e chiarimenti; ▪ monitora l'utilizzo delle TIC e segnala al DSGA eventuali problemi che dovessero richiedere acquisti o interventi tecnici; ▪ assicura che il personale possa accedere alla rete della scuola solo tramite password;

	▪ fornisce al personale, agli alunni e ai genitori consulenza e informazioni in relazione ai rischi on line e alle misure di prevenzione e gestione degli stessi; ▪ riceve segnalazioni di incidenti e-Safety e crea un registro degli incidenti e informa il DS.
5) DOCENTI	▪ danno chiare indicazioni sul corretto utilizzo della strumentazione multimediale, di internet, ecc.; ▪ segnalano prontamente eventuali malfunzionamenti o danneggiamenti al docente funzione strumentale; ▪ non divulgano le credenziali di accesso alla rete wifi; ▪ non salvano sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili; ▪ si informano/si aggiornano sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento; ▪ si assicurano che gli alunni seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet; ▪ controllano l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito); ▪ nelle lezioni in cui è programmato l'utilizzo di Internet, guidano gli alunni a siti controllati e verificati come adatti per il loro uso e controllano che nelle ricerche su Internet siano trovati e trattati solo materiali idonei; ▪ segnalano al Dirigente Scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme e/o stabiliscono comuni linee di intervento educativo per affrontarle;
6) IL PERSONALE ATA	▪ deve avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche; ▪ deve monitorare l'uso di dispositivi tecnologici e attuare politiche scolastiche per quanto riguarda questi dispositivi; ▪ deve segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o ai suoi collaboratori o alla Funzione Strumentale per le nuove tecnologie o all'Animatore Digitale per le opportune indagini / azioni / sanzioni;
7) GLI STUDENTI	▪ devono utilizzare le TIC su indicazioni del docente; ▪ devono, in caso di riscontro di malfunzionamenti della strumentazione e/o di contatto accidentale con informazioni, immagini e/o applicazioni inappropriate, comunicarlo immediatamente all'insegnante; ▪ non devono eseguire tentativi di modifica della 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 acquisito il permesso da parte dell'insegnante; ▪ devono chiudere correttamente la propria sessione di lavoro; ▪ devono essere consapevoli dei problemi di sicurezza connessi con l'uso di telefoni cellulari, telecamere e dispositivi portatili; ▪ devono essere responsabili dell'utilizzo delle attrezzature tecnologiche della scuola e comprendere l'importanza di

	adottare buone pratiche di e-Safety anche quando utilizzano tecnologie digitali fuori dalla scuola. ▪ devono avere una buona comprensione delle capacità di ricerca e della necessità di evitare il plagio e rispettare normative sul diritto d'autore; ▪ devono conoscere e capire l'azione educative della scuola sull'uso improprio di immagini e il cyberbullismo.
8) I GENITORI	▪ devono sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle Tecnologie dell' Informazione e delle Comunicazioni nella didattica; ▪ devono seguire gli alunni 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; ▪ devono 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.

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

Il presente documento sarà oggetto di condivisione e revisione da parte dell'intera comunità scolastica con il coinvolgimento di studenti, docenti e famiglie, con l'approvazione degli organi collegiali. La scuola si impegna a promuove eventi informativi e formativi, rivolti a tutto il personale, agli alunni e ai loro genitori, anche con il coinvolgimento di esperti.

Condivisione e comunicazione della Policy agli alunni:

- attraverso attività, laboratori, incontri, spettacoli che portino a riflettere sui rischi e opportunità del web.

Condivisione e comunicazione della Policy al personale:

- le norme adottate dalla scuola in materia di sicurezza nell'utilizzo del digitale saranno discusse negli organi collegiali e rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito web della scuola.

Condivisione e comunicazione della Policy ai genitori:

- le famiglie saranno informate in merito alla linea di condotta adottata dalla scuola per un uso sicuro e responsabile delle tecnologie digitali e di internet attraverso la condivisione del presente documento e di materiali informativi specifici sul sito web della scuola.

1.4. Gestione delle infrazioni della policy

Tutte le infrazioni alla presente Policy andranno segnalate al Dirigente Scolastico, che valuterà le possibili azioni da intraprendere. Verranno prese tutte le precauzioni necessarie per garantire la sicurezza on-line.

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

- un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare (cyberbullismo);
- l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;
- la condivisione di immagini intime o troppo spinte;
- il collegamento a siti web non indicati dai docenti.

Gli interventi correttivi previsti per gli alunni sono riferiti all'età e al livello di sviluppo cognitivo degli alunni. Sono previsti, quindi, provvedimenti disciplinari proporzionati all'età e alla gravità del comportamento, quali:

- il richiamo verbale;
- il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività);
- il richiamo scritto con annotazione sul diario;
- il ritiro del cellulare fino a fine giornata;
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente scolastico;
- la rimozione da internet o del computer di accesso per un periodo;
- comunicazioni alle autorità competenti;

Le denunce di bullismo online saranno trattate in conformità con la legge attuale (L.71/2017).
Sono anche previsti interventi di carattere educativo, di rinforzo dei comportamenti, correttivi e riparativi dei disagi causati, di promozione della conoscenza e della gestione delle emozioni, di prevenzione e gestione positiva dei conflitti, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di promozione di rapporti amicali e di reti di solidarietà, di moderazione dell'eccessiva competitività.

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

- una carente istruzione preventiva degli alunni sull'utilizzo corretto e responsabile delle tecnologie digitali e di internet;
- un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.

Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge.

Interventi sui genitori: Alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche verificatisi al di fuori del contesto scolastico. I genitori degli alunni possono essere convocati per concordare misure educative diverse, provvedimenti disciplinari oppure essere sanzionati a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

1.5. Monitoraggio dell'implementazione della Policy e suo aggiornamento

Il monitoraggio dell'implementazione della Policy verrà curato dal DS in collaborazione con le Funzioni Strumentali, l'Animatore Digitale e il Team dell'Innovazione che promuoveranno inoltre gli eventuali

aggiornamenti che si rendano opportuni, secondo una logica di condivisione con tutto il corpo docente e le famiglie.

1.6. Integrazione della Policy con documenti esistenti

Il presente documento si integra con gli obiettivi e i contenuti dei seguenti documenti:

- PTOF;
- Regolamento d'Istituto Sezione - Prevenzione e Contrasto del "Bullismo e Cyberbullismo",
- Patto Educativo di corresponsabilità.

2.1. Curricolo sulle competenze digitali per gli studenti

All'interno di un curricolo verticale esistente, l'Istituto è tenuto a sviluppare uno specifico curricolo finalizzato all'acquisizione di competenze digitali per gli studenti.
"La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet". Il Curricolo della scuola del primo ciclo di istruzione sulle competenze digitali per gli alunni è trasversale alle discipline previste dalle Indicazioni Nazionali: la competenza digitale è ritenuta dall'Unione Europea competenza chiave, per la sua importanza e pervasività nel mondo d'oggi. L'approccio per discipline scelto dalle Indicazioni non consente di declinarla con le stesse modalità con cui si possono declinare le competenze chiave nelle quali trovano riferimento le discipline formalizzate. Si ritrovano abilità e conoscenze che fanno capo alla competenza digitale in tutte le discipline e tutte concorrono a costruirla. Competenza digitale significa padroneggiare certamente le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con "autonomia e responsabilità" nel rispetto degli altri, sapendone prevenire ed evitare i pericoli. In questo senso, tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione e si perseguiranno 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 e riconoscerne le correlazioni e le conseguenze delle correlazioni;
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 coadiuvare la creatività e l'innovazione;
6. riflettere sulle problematiche legate alla validità e all'affidabilità delle informazioni disponibili;
7. acquisire consapevolezza sulle opportunità e sui potenziali rischi di Internet e della comunicazione tramite i supporti elettronici;
8. riflettere sui principi giuridici ed etici 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

I docenti hanno partecipato e parteciperanno a corsi di formazione e ad iniziative organizzate dalla stessa Istituzione scolastica e non; possiedono, in generale, una buona base di competenze e nel caso delle figure di sistema, anche di carattere specialistico. Il processo di formazione e aggiornamento è continuo, inesauribile nel tempo ed in rapporto al rinnovo della dotazione multimediale.
Lo sviluppo della tecnologia (più portatile, meno costosa e più diffusa) e i Piani Nazionali (LIM, Cl@assi 2.0 e PNSD) hanno permesso di portare con sempre maggiore costanza e diffusione le TIC a scuola ed hanno costretto modifiche nell'approccio metodologico–comunicativo da parte di tutti gli operatori scolastici.

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

delle Tic

Nell'ambito del PNSD la scuola ha previsto:

- ✓ individuazione e formazione di un Animatore Digitale che collaborerà col DS e il DSGA nell'attuazione degli obiettivi e delle innovazioni previste dal PSND;
- ✓ formazione dei docenti all'utilizzo del registro elettronico e dello scrutinio elettronico;
- ✓ ricognizione e messa a punto delle dotazioni digitali;
- ✓ somministrazione di un questionario rivolto ai docenti per la rilevazione dei " bisogni digitali";
- ✓ realizzazione/ampliamento della rete WI-FI/LAN di tutti plessi dell'Istituto;
- ✓ attivazione e comunicazione di iniziative di formazione/aggiornamento anche in materia di sicurezza online;

Allo scopo di promuovere la condivisione di buone pratiche per un uso consapevole e sicuro delle Tic e di prevenire e contrastare "ogni forma di discriminazione e del bullismo, anche informatico"- cyberbullismo (Legge 107/2015, art. 1, c. 7, l e Legge n. 71/2017) l'Istituto ha aderito, quest'anno, al progetto "Generazioni Connesse", percorso formativo online dove tutti i docenti sono invitati a riflettere sul loro approccio alle tematiche legate alle competenze digitali, alla sicurezza online e ad un uso positivo e consapevole delle tecnologie digitali nella didattica. Il sito fornisce tanti materiali che affrontano le problematiche e i rischi del web ma anche le sue potenzialità.

2.4. Sensibilizzazione delle famiglie

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.

L' Istituto attiva iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine organizza incontri fra docenti e genitori per la diffusione del materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati e dalle forze dell'ordine.

I docenti durante gli incontri scuola-famiglia suggeriscono la consultazione del portale www.generazioniconnesse.it 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.

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

L'infrastruttura e la strumentazione ICT dell'Istituto sono un patrimonio di tutti, esse vanno utilizzate nel rispetto delle norme contenute nel "Regolamento dell' Istituzione Scolastica per la gestione patrimoniale " e nel "Regolamento Laboratori e aule speciali". I danni causati alle attrezzature saranno a carico di chiunque disattenda i suddetti Regolamenti.
L'accesso ad infrastrutture e strumentazione ICT utilizzabili per la didattica è riservato agli insegnanti, agli alunni è limitato al perseguimento di scopi formativi. I docenti devono formare i propri alunni al rispetto del suddetto Regolamento, per gli aspetti di loro pertinenza.
L'Istituto è dotato di una rete wireless nei plessi della scuola secondaria e della scuola primaria L'accesso a internet è consentito a scopi didattici al personale docente attraverso l'assegnazione di una password comune a tutti. 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 devono mai comunicare la password di accesso.

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

L'accesso al sistema informatico, server e internet nel laboratorio multimediale è consentito al personale docente, solo per fini didattici e attraverso l'assegnazione di una password. La password è comune e consente di accedere al server. I docenti registrano il proprio accesso, scrivendo su un registro la data e l'orario di utilizzo del laboratorio. Non vi è un backup dei file elaborati, se non quello operato dai docenti interessati sui supporti rimovibili personali (pendrive, hard disk esterni, o altro). Le postazioni del laboratorio funzionano come stazioni di lavoro e non come archivi.
Si ribadisce che agli studenti non è consentito accedere ad Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto. L'uso di cellulari è vietato come da Regolamento.

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, sia nella versione posta ordinaria che certificata. L'eventuale invio o ricevimento di posta a scopi didattici, sarebbe svolto dall'assistente amministrativo addetto. La posta elettronica è protetta da antivirus e quella certificata anche dall'antispam. Le circolari, le informazioni principali, le convocazioni vengono diramate esclusivamente tramite posta elettronica.

3.4. Sito web della scuola

La scuola ha un sito web e un proprio dominio : https://www.iissarena.gov.it/
Tutti i contenuti del settore didattico sono pubblicati direttamente e sotto supervisione del Dirigente Scolastico che ne valuta la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy ecc, secondo le disposizioni normative.

3.5. Social network

Attualmente nella didattica non si utilizzano social network, né l'Istituzione scolastica vi ha creato una pagina col proprio profilo o ha autorizzato il personale scolastico a utilizzarli per nome e per conto della stessa. Per la Legge l'utilizzo dei Social Network con la pubblicazione di nomi e giudizi sulle persone o sulle istituzioni e la diffusione di foto/filmati senza il consenso e, comunque, all'insaputa delle persone coinvolte può determinare ricadute di carattere anche penale, come ad esempio la diffamazione. Si invitano, pertanto, tutti gli studenti a non prelevare o diffondere immagini, video o registrazioni – anche solo audio – non autorizzate, ed eliminare da internet eventuali riferimenti illeciti, inopportuni e offensivi nei confronti dell'Istituto e della sua comunità scolastica. Tali giudizi, una volta pubblicati, comportano sempre una assunzione di responsabilità da parte di chi li ha scritti o anche semplicemente diffusi.

3.6. Protezione dei dati personali

Il personale scolastico è incaricato del trattamento dei dati personali degli alunni, dei genitori, ecc. (Legge 675/96 e successive modifiche ed integrazioni) nei limiti delle operazioni di trattamento e delle categorie di dati necessari ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Tutto il personale incaricato riceve poi 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, fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori per un loro eventuale utilizzo a scopi didattici, informativi e divulgativi anche tramite pubblicazione su siti web.

4.1. Per gli studenti

È vietato l'utilizzo di cellulari e di smartwatches per l'intera durata delle attività scolastiche. La normativa vigente stabilisce che non è consentito agli alunni l'uso del cellulare in orario scolastico, intervalli compresi, per ricevere o effettuare chiamate, messaggi o per chattare (Dpr 249/1998, Dpr 235/2007, DM 15/03/2007). Per gli alunni con disabilità, con disturbi specifici di apprendimento, BES, previa consultazione con il consiglio di Classe, si concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili e le modalità di custodia. Gli insegnanti di classe avranno cura di vigilare sul corretto utilizzo di tali dispositivi.

In caso di violazione delle suddette disposizioni, sarà previsto il ritiro temporaneo dei dispositivi da parte del docente che rileva la violazione. Gli strumenti non permessi saranno depositati nella cassaforte della scuola e successivamente consegnati al genitore/tutore convocato, che sarà contestualmente **informato dell'eventuale sanzione disciplinare comminata al trasgressore.**

Nel caso in cui gli alunni debbano comunicare con la famiglia durante l'orario scolastico, possono usare la linea fissa della scuola; allo stesso modo le famiglie devono chiamare la scuola se hanno assoluta necessità di parlare con i propri figli. Si raccomanda di ridurre tali comunicazioni a casi di necessità e urgenza.

Ai sensi della Direttiva Ministeriale n. 30 del 15 marzo 2007, 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.

4.2. Per i docenti: gestione degli strumenti personali – cellulari, tablet ecc.

Durante le ore di lezione è consentito ai docenti l'uso di dispositivi elettronici personali a scopo didattico e a integrazione dei dispositivi scolastici disponibili (es. il computer di classe). Non è possibile utilizzare cellulari e smartphone per attività personali e che esulino dall'insegnamento. Durante il restante orario di servizio, l'uso del cellulare è consentito per comunicazioni personali che rivestano carattere di urgenza. L'uso di altri dispositivi elettronici personali è possibile per attività funzionali all'insegnamento.

4.3. Per il personale della scuola

Durante l'orario di servizio è consentito al personale scolastico l'uso di cellulari e smartphone per comunicazioni personali urgenti. L'uso di altri dispositivi elettronici personali o dell'Istituto è consentito solo per attività funzionali al servizio.

Nell'invitare tutta la comunità scolastica (studenti, docenti, personale ATA e famiglie) ad evitare, per quanto non necessario, la pubblicazione in rete di immagini e/o video ripresi all'interno dell'Istituto (fatta salva la pubblicazione a scopi didattici, previa informativa al Dirigente Scolastico), è bene ricordare che, secondo la normativa vigente, non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese e che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere in gravi violazioni, incorrendo in sanzioni disciplinari, pecuniarie ed eventuali reati.

5.1. Prevenzione

Contrastare il bullismo implica la creazione di una comunità solidale, in cui ogni allievo accetta sia il

diritto di vivere una scuola senza violenza, sia la responsabilità di difendere i compagni più vulnerabili. Il coinvolgimento dei coetanei è indispensabile per creare un clima di solidarietà, combattere l'omertà e l'indifferenza, incoraggiare le vittime a chiedere aiuto, sottrarre al bullo i potenziali proseliti.

Rischi

Al personale che opera nella scuola e in modo particolare agli insegnanti, viene oggi data la facoltà di essere promotori e garanti della costruzione dialogica di un percorso formativo partecipato e il loro ruolo può diventare quello di confidenti degli alunni e delle loro esperienze. Proprio per questo, gli insegnanti devono essere bravi a individuare i "campanelli d'allarme" o meglio le problematiche o i rischi che bambini e adolescenti possono trovarsi ad affrontare ogni giorno, dunque devono imparare a riconoscere *i rischi* più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente. Tra questi, un'attenzione specifica andrà prestata alla:

- possibile esposizione a contenuti violenti 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-grooming);
- rischio di molestie o maltrattamenti da coetanei (cyber-bullismo);
- scambio di materiale a sfondo sessuale (sexting);
- uso eccessivo di Internet/cellulare (dipendenza).

Azioni

Premesso che non ci sono ricette sicure per eliminare il (cyber)bullismo, la Scuola ha scelto di impegnarsi su più fronti per essere quanto più possibile zona libera da (cyber)bullismo. Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli studenti in orario scolastico, sono state realizzate o programmate le seguenti:

- diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web, condividendo materiali messi a disposizione sul sito del progetto "Generazioni connesse";
- far rispettare il divieto di utilizzo di dispositivi digitali propri, quali cellulare e smartphone, agli studenti in orario scolastico;
- impedire un utilizzo incauto, scorretto o criminoso degli strumenti digitali sui dispositivi in uso a scuola (principalmente pc) sono:
- bloccare l'accesso a un sito o a un insieme di pagine impedendone la consultazione;
- controllare periodicamente i siti visitati dagli alunni;
- utilizzare filtri, software che impediscono il collegamento ai siti web per adulti (black list);
- utilizzare un software in grado di intercettare le richieste di collegamento e di respingere quelle non conformi alle regole stabilite dall'amministratore;
- fornire ai genitori informative 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);
- implementare la eSafety Policy con il contributo di tutte le componenti (docenti, studenti, famiglie, personale A.T.A.);
- presentare la eSafety Policy così redatta agli Organi Collegiali e quindi inserirla nel sistema di regolamenti della Scuola e renderla pubblica sul sito della Scuola.

5.2. Rilevazione

Cosa segnalare

Si considerano da segnalare tutte quelle situazioni 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.
Può capitare che un alunno manifesti un'insofferenza nei confronti di un compagno o, al contrario, che un alunno si senta escluso o emarginato dai coetanei. In alcuni casi sono gli alunni stessi a rivolgersi ai docenti in cerca di aiuto, anche quando i fatti siano accaduti fuori dall'ambiente e dall'orario scolastico.
La diffusione capillare dei social network tra i bambini e ancor più tra gli adolescenti li espone sempre più spesso al rischio di inviare o condividere senza alcuna protezione materiali personali o riservati.
Discutendo in classe dei rischi del web e confrontandosi sulle esperienze personali o dei propri coetanei, emergono spesso fatti che "allarmano" l'insegnante. Tra i contenuti andranno opportunamente segnalati:
- dati sensibili o riservati (foto, immagini, video personali, informazioni private proprie o di amici; l'indirizzo di casa o il telefono, ecc.);
- contenuti che possano considerarsi in qualche modo lesivi dell'immagine altrui (commenti offensivi, minacce, osservazioni diffamatorie o discriminatorie, foto o video denigratori, videogiochi che contengano un'istigazione alla violenza, ecc.);
- contenuti riconducibili alla sfera sessuale: messaggi, immagini o video a sfondo sessuale, come foto di nudo o semi-nudo, ecc.

Come segnalare: quali strumenti e a chi

Il responsabile di rete e della connessione dovrà provvedere a conservare le eventuali tracce di una navigazione non consentita su internet o del passaggio di materiali inidonei sui pc della scuola; la data e l'ora consentiranno di condurre più approfondite indagini; nel caso di messaggi, si cercherà di risalire al mittente attraverso i dati del suo profilo. Sia nel caso di chat che di messaggi di posta elettronica, l'insegnante, ove possibile, dovrà copiare e stampare i messaggi per fornire le eventuali prove dell'indagine sugli abusi commessi. Tali prove saranno utili anche ad informare la famiglia dell'alunno vittima di abuso, il Dirigente scolastico e, ove si configurino reati, la Polizia Postale. In ogni caso, sarà opportuna una tempestiva informazione delle famiglie in merito all'accaduto, anche per consentire ulteriori indagini e, in assenza di prove oggettive, di raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico ed, eventualmente, alla Polizia Postale. Qualora siano coinvolti più alunni, in qualità di vittime o di responsabili della condotta scorretta, le famiglie degli alunni in questione saranno informate tempestivamente per un confronto.
Quindi in base all'entità dei fatti si provvederà:

1. ad un'annotazione del comportamento sul registro;
2. ad una comunicazione scritta alle famiglie che la devono restituire vistata;
3. ad una convocazione formale dei genitori degli alunni, tramite segreteria;
4. ad una convocazione delle famiglie da parte del Dirigente scolastico;
5. ad una relazione scritta al Dirigente scolastico.
6. alla compilazione di un "diario di bordo" della scuola nel quale riportare le situazioni problematiche online che vengono affrontate;
7. ad un utilizzo di una "mappa" che propone alcuni step da seguire per intervenire in modo tempestivo ed efficace qualora si venga a conoscenza di situazioni di pregiudizio che i propri alunni vivono sul web.

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). In particolare per i fatti criminosi, ai fini della denuncia, la relazione deve essere redatta nel modo più accurato possibile, indicando i seguenti elementi: il fatto, il giorno dell'acquisizione del fatto nonché le fonti di prova già note e per quanto possibile, le generalità, il domicilio e quant'altro di utile a identificare la persona alla quale il reato è attribuito, la persona offesa e tutti coloro che sono in grado di riferire circostanze rilevanti per la ricostruzione del fatto.

5.3. Gestione dei casi

Casi di cyberbullismo:

Si definiscono atti di bullismo tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o a volte un piccolo gruppo). Si tratta, pertanto, di una serie di comportamenti portati avanti ripetutamente nel tempo. Si parla di cyberbullismo quando queste forme di prevaricazione reiterate nel tempo si estendono anche alla vita online. I comportamenti cosiddetti "quasi aggressivi", che spesso si verificano tra coetanei, le interazioni animate o i contrasti verbali, o la presa in giro "per gioco", effettuata anche in rete, mettono alla prova la relazione con i compagni, la supremazia o la parità tra i soggetti implicati e l'alternanza e sperimentazione dei diversi ruoli. Il gruppo dei pari rappresenta anche il momento di conquista dell'autonomia dall'adulto e pertanto luogo di "complicità" e di piccole "trasgressioni", di scambi "confidenziali" condivisi fra gli amici nella rete o con il cellulare. Detti comportamenti, che finiscono per arrivare all'attenzione degli adulti, sono controllati e contenuti dai docenti attraverso i normali interventi educativi, di richiamo al rispetto delle regole di convivenza civile e democratica, di rispetto degli altri, per evitare che possano degenerare, diventare pericolosi per sé o offensivi e minacciosi per gli altri.

Gli interventi mirati sul gruppo classe sono gestiti in collaborazione dal team dei docenti della classe e d'intesa con le famiglie, ad esempio con percorsi di mediazione volta alla gestione positiva del conflitto, con gruppi di discussione (circle time), con rappresentazioni e attività di role-play sull'argomento, con le strategie del problem solving. Vengono intrapresi anche i 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 smuoverne le competenze empatiche e a favorire una loro condivisione delle norme morali.

Genericamente, si sottolinea che il bullismo ha caratteristiche peculiari:

- è pervasivo: il bullo può raggiungere la sua vittima in qualsiasi momento e in qualunque luogo;
- è un fenomeno persistente: il materiale messo online vi può rimanere per molto tempo;
- spettatori e cyberbulli sono potenzialmente infiniti: le persone che possono assistere agli atti di cyberbullismo sono potenzialmente illimitate. Occorre tenere presente che il cyberbullo non è mai del tutto consapevole della gravità dei suoi comportamenti se non viene aiutato ad esserne consapevole.

Qualora ci si trovi di fronte ad un caso di cyberbullismo si dovrà:

- informare i genitori degli alunni coinvolti;
- coinvolgere il referente d' Istituto dell'e-safety e gli operatori scolastici su quanto sta accadendo;
- coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online;
- tenere traccia di quanto successo e delle azioni intraprese, compilando un "diario di bordo" per consentire ulteriori indagini se necessarie.

Casi di sexting

Qualora ci si trovi di fronte a un caso di sexting (con cui si intende l'invio e/o la ricezione e/o la condivisione di testi, video o immagini sessualmente esplicite via cellulare o tramite internet) si dovrà:

- coinvolgere la classe e confrontarsi con esperti, facendo appello, per esempio, allo sportello d'ascolto dell'Istituto (se attivo) per capire come approfondire e affrontare il fenomeno;
- coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti riconducibili al sexting;
- documentarsi opportunamente sulle norme giuridiche che regolano i comportamenti e le condotte sessuali in Italia;
- intraprendere con la classe attività mirate a riflettere sulla fiducia che ciascuno ripone negli altri e sul fenomeno del sexting, approfondendo casi e testimonianze.

Casi di adescamento online o grooming

Le tecnologie digitali consentono ai giovani di ampliare la propria rete di amicizie in modo quasi smisurato: non di rado i bambini "concedono" la loro amicizia non solo a persone che conoscono direttamente, ma anche ad "amici di amici". Spesso l'adulto finge di essere minorenne. Questo li espone

a rischi notevoli, come quello di dare accesso a sconosciuti al loro mondo online e quindi a informazioni personali. È bene che anche gli insegnanti aiutino i propri alunni a tutelarsi, scegliendo con cura chi frequentare online, per evitare che una condotta imprudente possa comportare ripercussioni non banali nella loro vita reale. Una volta riconosciuti alcuni segni che possono rinviare a una situazione di adescamento online, quali un improvviso calo nel rendimento scolastico, un aumento del tempo trascorso dall'alunno online congiunto ad una particolare riservatezza al riguardo, allusioni da parte dell'alunno alla frequentazione di una persona più grande o a regali ricevuti ecc., è bene:
- approfondire la situazione coinvolgendo la classe e l'intera comunità scolastica;
- avviare dei percorsi di riflessione in classe sul concetto di fiducia;
- farsi affiancare da esperti, ricorrendo anche allo sportello d'ascolto per offrire ai minori, qualora lo desiderino, il supporto necessario, uno sportello attivo e disponibile quotidianamente, gestito da personale competente, qualificato e finanziato;
- contattare direttamente una helpline.

La denuncia all'autorità giudiziaria o agli organi di Polizia, da parte degli insegnanti o del Dirigente scolastico, costituisce il passo necessario per avviare un intervento di tutela a favore della vittima e attivare un procedimento penale nei confronti del presunto colpevole. La presa in carico di situazioni di abuso sessuale, così delicate e complesse, richiede un approccio multidisciplinare, da parte di diverse figure professionali. I versanti su cui si articola l'intervento possono essere essenzialmente tre: medico, socio-psicologico e giudiziario. Il compito della scuola non è comunque solo quello di "segnalare" ma, più ampio ed importante, nella ripresa della piccola vittima, in quanto ha al suo interno fattori relazionali ed educativi che possono aiutare il bambino a riprendere una crescita serena. A tal fine la scuola lavora insieme alle altre figure professionali e alle famiglie, scambiando informazioni e condividendo progetti e prassi operative, favorendo le occasioni di confronto e di dialogo.

Annessi

1. **Procedure operative per la gestione dei casi (adescamento o grooming)**

Cosa fare se un alunno/a viene adescato/a on-line:

- la situazione richiede delicatezza: cercare di capire meglio cosa sta succedendo;
- coinvolgere i genitori, anche se chi è coinvolto se ne vergogna ed è restio a farlo;
- informare il referente di Istituto e-safety e gli operatori scolastici;
- se è opportuno, richiedere un supporto ai servizi territoriali o ad altre Autorità competenti;
- effettuare una segnalazione alla polizia postale affinché rintraccino e blocchino l'adescatore;
- se i contenuti sono online segnalare per rimuoverli ai servizi di Generazioni Connesse;
- se la classe ne è a conoscenza, responsabilizzare i propri alunni: chiedendo che supportino la vittima senza prenderla in giro;
- deresponsabilizzare la vittima: spesso si sente in colpa per quanto accaduto;
- dialogare (con la classe – 1) parlare della necessità di non fidarsi: in rete non sempre si è chi si dice di essere. Informare sulle leggi in materia di adescamento;
- prevenire (con la classe – 2) proporre discussioni/attività sulla fiducia e sull'uso consapevole del web;
- quando i contenuti sono rimossi/cancellati, coinvolgere il team e-safety sulle azioni appropriate per prevenire altre situazioni di rischio;
- coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online;
- tenere traccia di quanto accaduto e delle azioni intraprese: compilare il diario di bordo.

2. **Procedure operative per la gestione delle infrazioni alla Policy.**

- Le segnalazioni di un uso improprio di Internet saranno trattate dal responsabile e-safety.
- Qualsiasi denuncia di abuso personale deve essere riferito al Dirigente Scolastico.

- Le segnalazioni che riguardano la protezione dei minori devono essere trattate in conformità con procedure di protezione degli alunni della scuola.
- Gli alunni e genitori devono essere informati delle procedure di segnalazione.
- Eventuali casi di infrazioni alla Policy verranno comunicati alle forze dell'ordine ai servizi del territorio al fine di stabilire procedure per la gestione di questioni potenzialmente illegali.

3. Procedure operative per la protezione dei dati personali.

In ottemperanza al codice sulla privacy (Decreto Legislativo n. 196/2003, codice in materia di protezione dei dati personali) tutti i dati personali degli alunni oggetto di trattamento sono:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- conservati in una forma che consenta l'identificazione dell'alunno per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Si allegano schede operative fornite dalla piattaforma "Generazioni connesse" per la rilevazione e la estione dei casi.

ALLEGATI:

- All. 1: Diario di bordo per il monitoraggio delle situazioni a rischio
- All. 2: Mappa "Cosa fare in caso di…"
- All. 3: Schema di segnalazione alunno
- All. 4: Scheda per la rilevazione di violazione delle disposizioni sulla strumentazione personale
- All. 5: Liberatoria per l'utilizzo delle immagini
- All. 6: Format di segnalazione al servizio sociale territoriale
- All. 7: Format per la segnalazione all'autorità giudiziaria
- All. 8: Vademecum per i genitori sull'uso sicuro del telefonino da parte dei minori
- All. 9: Glossario

- **All. 1: Diario di bordo per il monitoraggio delle situazioni a rischio**

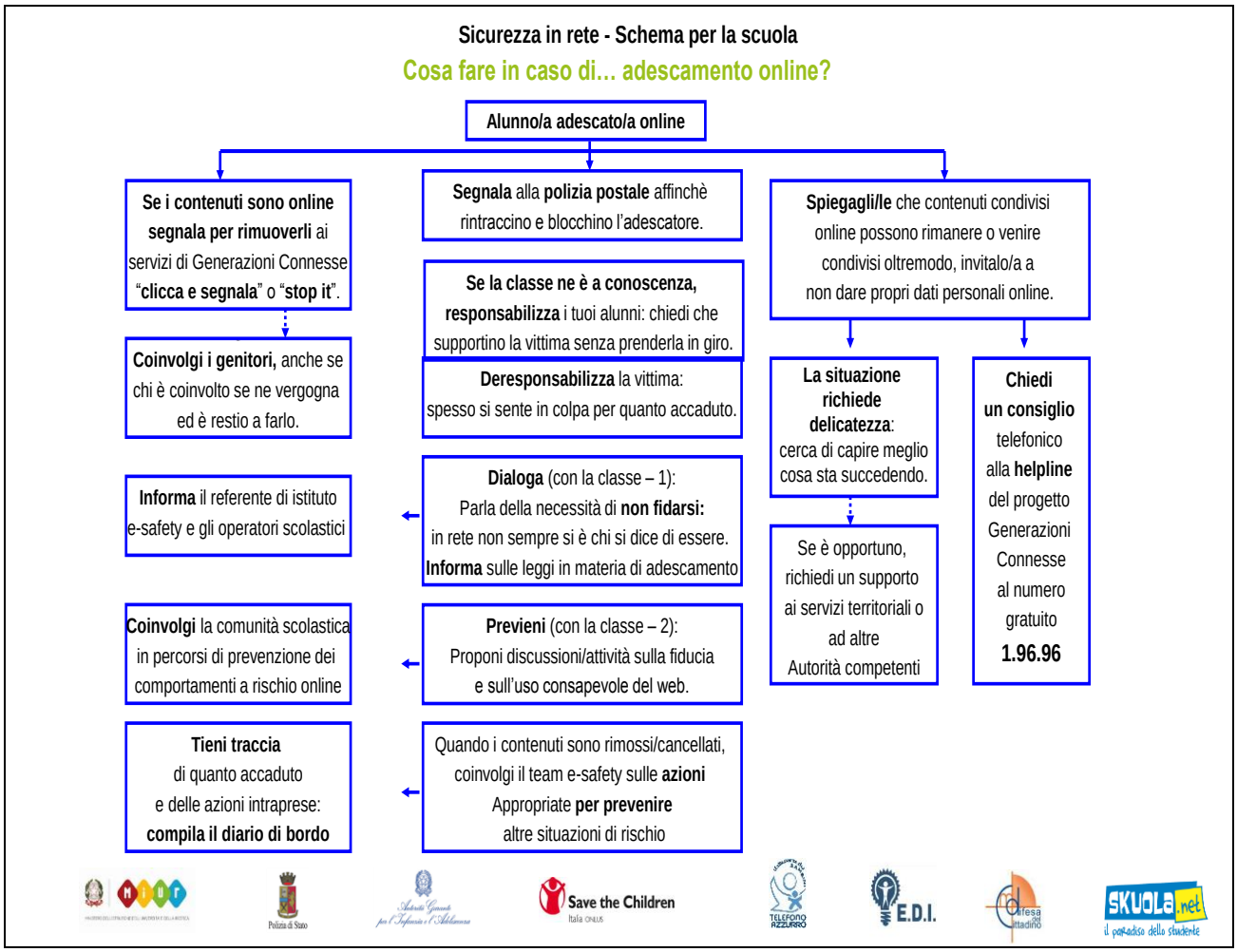
Riepilogo casi

Scuola_____

Anno Scolastico_____

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

All. 2: Mappa "Cosa fare in caso di…"



All. 3: Schema di segnalazione alunno

SCHEDA DI SEGNALAZIONE		
ALUNNO		
CLASSE	*SEZIONE*	
PLESSO		
OSSERVAZIONE DIRETTA	***EVENTO RIFERITO***	***DESCRIZIONE***
☐	☐	Esposizione a contenuti violenti
☐	☐	Uso di videogiochi diseducativi
☐	☐	Accesso ed utilizzo di informazioni scorrette o pericolose
☐	☐	Scoperta ed utilizzo di virus in grado di infettare computer
☐	☐	Possibile adescamento
☐	☐	Cyberbullismo (rischio di molestie o maltrattamenti da coetanei)
☐	☐	Sexting (scambio di materiale a sfondo sessuale)
☐	☐	Dipendenza da uso eccessivo
Firma docente		

All. 4: Scheda per la rilevazione di violazione delle disposizioni sulla strumentazione personale

SCHEDA PER LA RILEVAZIONE DI VIOLAZIONE DELLE DISPOSIZIONI SULLA STRUMENTAZIONE PERSONALE	
ALUNNO	
CLASSE	*SEZIONE*
PLESSO	
DOCENTE/I COINVOLTO/I	
DATA DELLA VIOLAZIONE	
DESCRIZIONE DEI FATTI	
Firma docente/i coinvolto/i	

All. 5: Liberatoria per l'utilizzo delle immagini

DICHIARAZIONE LIBERATORIA DEI GENITORI/TUTORI PER LA PUBBLICAZIONE DI ELABORATI, NOMI, VOCI, IMMAGINI, MATERIALE AUDIOVISIVO

Al Dirigente Scolastico
dell'II.SS Don Michele Arena
di Sciacca

Oggetto: **Liberatoria per l'utilizzo delle immagini.**

DATI DELL'ALUNNO

Cognome _____ Nome_____

nato/a _____ il _____

Scuola _____ classe _____ sez._____

DATI DEL GENITORE

_L_sottoscritt _____

con la presente AUTORIZZA l'utilizzo delle immagini registrate nell'ambito delle attività/progetti realizzati dall'istituzione Scolastica, con diffusione sulle piattaforme digitali e in televisione, nel pieno rispetto della funzione educativa degli interventi. La posa e l'utilizzo delle immagini sono da considerarsi effettuate in forma gratuita.

Sciacca, li

Firma del genitore

_____

All. 6: Format di segnalazione al servizio sociale territoriale

Al Servizio Sociale Territoriale

del Comune di _____

Oggetto: Segnalazione relativa al minorenne

Nome e Cognome ……

nato/a ..... il ……

Figlio/a di …… e di .....…….

Residente a ……. in via …….....….....

La relazione deve contenere le seguenti informazioni:

1. Dati anagrafici del minorenne e del nucleo familiare;
2. Descrizione generale della situazione di rischio individuata dagli scriventi [CHI, COSA, DOVE, QUANDO] (attenersi il più possibile ai fatti, riportando tra virgolette il linguaggio utilizzato dal minorenne);
3. Descrizione nel dettaglio del/degli episodi ritenuti particolarmente significativi (breve resoconto di un colloquio, presenza di disegni, comportamenti critici rilevanti);
4. Descrizione di eventuali colloqui con i familiari e degli interventi effettuati a favore del minorenne all'interno della scuola e/o dai servizi sociali (se conosciuti). Si ricorda che nei casi di sospetto abuso sessuale onlìne intrafamiliare e di grave pregiudizio intrafamiliare NON VA CONVOCATA NE' AVVISATA LA FAMIGLIA.

Luogo e Data, …….

Firma

_____

All. 7: Format per la segnalazione all'autorità giudiziaria

Data, Luogo ……..

Prot. n. [FACOLTATIVO]

Spett. le Procura della Repubblica
c/o Tribunale per i Minorenni
e
Spett. le Procura della Repubblica
c/o Tribunale Ordinario

Per gli adempimenti del caso, s'invia scheda di segnalazione riguardo al minorenne:

Nome …… Cognome …….....

Sesso ☐ M ☐ F Luogo e data di nascita ……..……..

Indirizzo …….....

Composizione nucleo familiare ……...

Generalità dei genitori …….....

……

ELEMENTI DI PREOCCUPAZIONE CHE RENDONO NECESSARIA LA SEGNALAZIONE (CHI, COSA, DOVE, QUANDO) …...……..……

…….

Sono stati riscontrati danni fisici/psicologici sul minorenne ☐ Si ☐ No

Refertati da……..…….…….....

Che cosa si riscontra: ……..…….....

LA SITUAZIONE E' GIÀ A CONOSCENZA DEI SERVIZI SOCIALI ☐ Si ☐ No

Servizio ……...Per quale motivo …….……

Operatore di riferimento…….…….....

FIGURE DI RIFERIMENTO PER IL MINORENNE

- Genitore ……...
- Parenti (specifica) ……..
- Altro ……

La presente scheda può essere compilata anche parzialmente con le informazioni a conoscenza del segnalante.

Luogo e Data …….. Firma

……..

All. 8: Vademecum per i genitori sull'uso sicuro del telefonino da parte dei minori

- Spiega a tuo figlio che il telefonino è un mezzo di comunicazione che impone una cautela analoga a quella che si ha nei confronti del computer. Scegli per i più piccoli modelli semplici, quelli con telecamere e fotocamere riservali quando sapranno utilizzarli in modo sicuro e consapevole.
- Spiega a tuo figlio che foto e riprese effettuate con il telefonino sottostanno alla normativa italiana in materia di protezione dell'immagine e della privacy delle persone.
- Per i telefonini che consentono la navigazione in Internet o l'accesso a community e chat, spiega a tuo figlio che i rischi in termini di adescamenti da parte di pedofili on-line sono i medesimi della "Rete tradizionale".
- Scegli per i tuoi figli SIM Card ricaricabili e ricarica sempre tu il credito in modo da poter monitorare la quantità di traffico telefonico effettuato.
- Al momento dell'attivazione della SIM Card fornisci ai tuoi figli il PIN ma non il PUK. Con il PUK infatti potrai accedere al telefono anche se il PIN è stato modificato.
- Spiega ai tuoi figli che sms o mms che promettono ricariche facili o altri vantaggi immotivati sono spesso il primo contatto effettuato da chi non ha buone intenzioni.
- Parla ai tuoi figli della potenziale pericolosità di richiamare con il telefono numeri sconosciuti da cui provengono squilli o chiamate mute. In passato si è trattato di una modalità con cui i pedofili adescavano i minori.
- Scoraggia tuo figlio dal diffondere foto o filmati con il telefonino in community o chat telefoniche. Una volta immesse in Rete foto e filmati possono continuare ad essere diffuse senza controllo per lungo tempo.

All. 9: Glossario

ADWARE: Particolare versione di spyware atto a monitorare informazioni personali o sensibili a fini pubblicitari.

ANTISPAM: Programma o tecnologia che impedisce, o quantomeno limita, la ricezione di posta indesiderata nella propria casella di posta in entrata.

ANTISPYWARE: Il software antispyware protegge il computer da popup pubblicitari, lentezza e minacce alla sicurezza dovute a spyware e altro software indesiderato.

ANTIVIRUS: Programma che individua, previene e rimuove programmi dannosi, come virus e worm. Affinché sia efficace deve essere costantemente aggiornato.

ATTIVAZIONE: Procedura indispensabile, connessa all'installazione di molti software per attestarne la genuinità.

BACKDOOR: Accesso abusivo a un sistema informatico. Di solito una backdoor viene inserita dagli stessi programmatori del sistema per poter effettuare accessi di emergenza, ma a volte gli hacker riescono a individuarle sfruttandole a proprio vantaggio.

BACKUP: Operazione che consiste nel salvare periodicamente i dati memorizzati sul disco fisso del PC. È indispensabile fare backup frequenti perché un virus, un guasto dell'hardware, un incendio o anche un'operazione sbagliata possono causare la perdita dei dati.

BOT: Il termine bot è un'abbreviazione di "robot". I pirati informatici li usano per trasformare il tuo computer in un dispositivo in grado di effettuare automaticamente operazioni su Internet a tua insaputa.

CHAT: Significa "chiacchierare" e indica le conversazioni scritte in tempo reale che si possono fare in rete con altri utenti tramite appositi programmi per esempio Messenger e Skype. Nelle versioni più evolute le Chat prevedono la possibilità di parlare sfruttando microfono e casse del PC o addirittura di effettuare video conversazioni.

CLOUD: Il termine inglese cloud computing indica un insieme di tecnologie che permettono di memorizzare ed elaborare dati grazie all'utilizzo di risorse hardware e software distribuite e virtualizzate in Rete. SkyDrive e le Office Web Apps sono un esempio di servizio cloud offerto gratuitamente da Microsoft.

CONTROLLO ACTIVEX: I controlli ActiveX sono piccoli programmi che vengono utilizzati su Internet. Nella maggior parte dei casi sono utili, per esempio per l'installazione di aggiornamenti di sicurezza, ma se usati illegalmente possono effettuare attività senza il tuo controllo.

COOKIE: I Cookie sono piccoli file che i siti web salvano sul tuo disco rigido alla tua prima visita. Il loro compito è quello di ricordare i tuoi dati quando ritorni a visitare un sito. Generalmente i cookie non sono dannosi, ma se usati in maniera fraudolenta possono sottrarre informazioni a tua insaputa.

COPYRIGHT: È il diritto d'autore che stabilisce la proprietà intellettuale di un'opera.

CRACCARE: Neologismo gergale da "to crack", "spezzare". Si intende il superamento delle protezioni di un programma o di un sistema informatico.

CRACK: Un sistema generalmente software, in grado di eliminare le protezioni che vengono normalmente applicate ai programmi per evitare che vengano duplicati e installati illecitamente. L'utilizzo dei crack è illegale.

CRACKER: Declinazione negativa dell'hacker. Quest'ultimo generalmente viola i sistemi informatici solo per metterli alla prova, mentre il Cracker lo fa con l'obiettivo di sottrarre i dati, danneggiare i sistemi o sottrarre denaro, per esempio da un conto corrente on line.

CYBERBULLISMO: Termine che identifica attività di bullismo perpetrate tramite internet. Segnala l'episodio di bullismo al sito Web in cui è avvenuto. Molti servizi si avvalgono di moderatori e di luoghi in cui segnalare gli abusi, ad esempio abuseramicrosoft.com.

CYBERPEDOFILIA: Il pedofilo telematico è un individuo estremamente pericoloso perché spesso è difficile da individuare. Tipicamente cerca di instaurare un clima di fiducia e di amicizia fingendosi coetaneo dei bambini e cercando di agire quando il minore non è controllato da persone adulte.

DIALER: È uno speciale programma auto-eseguibile che altera i parametri della connessione a internet impostati sul computer dell'utente, agendo sul numero telefonico del collegamento e sostituendolo con un numero a pagamento maggiorato su prefissi internazionali satellitari o speciali.

DISCLAIMER: Significa "Esonero di responsabilità". L:insieme dei diritti e doveri dell'utente e limitazioni di responsabilità del produttore, relative a un software, da accettare al momento dell'installazione.

DRM: Acronimo di Digital Right Management, standard ideato da Microsoft sulla gestione dei diritti relativo alle opere digitali protette da copyright.

FAKE: Identifica un falso, Su Internet usato spesso per identificare l'utilizzo di un'identità falsa o altrui, un file fasullo o un allarme relativo a un virus inesistente.

FILE SHARING: Scambio di file solitamente attraverso reti paritarie [p2pl, ma anche attraverso apposite piattaforme. Può essere illegale.

FILTRO SMART SCREEN: Il filtro SmartScreen è una funzionalità di Internet Explorer 9 e 8 che ti aiuta a evitare le minacce di ingegneria sociale, sotto forma di malware e phishing, e le truffe on line quando navighi sul web.

FIREWALL: Un firewall è un programma software o un componente hardware che permette di respingere gli attacchi di hacker, virus o worm che cercano di raggiungere il computer attraverso internet.

FIRMA DIGITALE: Procedura che garantisce l'integrità e l'autenticità di un documento informatico, in analogia con la firma autografata.

FLAME: Il termine significa "fiammata" ed è tipico dei newsgroup. Identifica un attacco o reazione aggressiva verbale nei confronti di un utente.

FURTO DI IDENTITÀ: Il furto di identità è un qualsiasi tipo di frode che porta alla perdita di dati personali,come password, nomi utente, dati bancari o numeri di carte di credito. La forma più diffusa è il phising, ovvero la frode perpetrata tramite mail.

HACKER: Nella sua forma più pura si può considerare una sorta di studioso dei sistemi informati ci, che tenta di violare per saggiarne i limiti e la sicurezza senza provocare danni. Purtroppo sempre più spesso gli hacker diventano cracher, ovvero persone che lo fanno a scopo di lucro, per sottrarre dati o per mettere fuori uso i sistemi informatici.

HTTPS: l'utilizzo del protocollo HTTPS [Hyper text Transfer Protocol Securel consente di proteggere le informazioni inviate in Internet. In Hotmail viene per esempio utilizzato il protocollo HTTPS per la crittografia delle informazioni di accesso.

ICRA: Internet Contant Rating Association. Un'associazione internazionale senza fini di lucro nata per difendere e aiutare la navigazione dei minori in Rete.

INPRIVATE BROWSING: Tecnologia che consente di evitare che la cronologia delle esplorazioni, i file internet temporanei, i dati dei moduli, i cookie nonché i nomi utente e le password vengano mantenuti nel browser. In questo modo non lascerai traccia della tua navigazione.

LOGIN: Procedura di accesso a un computer, a un programma o a un servizio, generalmente legata all'inserimento di un username e di una password. È fondamentale scegliere password sicure per evitare che altri possano accedere senza il nostro consenso,

LURKER: Chi sta in agguato. Nelle attività in rete indica chi osserva senza prendere parte attiva.

MALWARE: Malware è l'abbreviazione di "maliciuous software", ovvero software dannoso. Con questo termine si identifica un software che viene installato senza il tuo consenso, per esempio mentre scarichi un programma gratuito o un file da una rete peer to peer.

MICROSOFT SECURITY ESSENTIALS: Microsoft Security Essentials è un software antimalware gratuito per il tuo computer. Ti protegge da virus, spyware e altro malware. È scaricabile gratuitamente per Windows 7, Window Vista e Windox XP SP2 e superiori.

NETIQUETTE: Contrazione di Net Etiquette, ovvero "etichetta di rete". Insieme di regole che disciplinano il comportamento di un utente in internet. Il rispetto della netiquette non è imposto da alcuna legge, ma è prassi comune attenervisi.

NETIZEN: Il termine significa "cittadino della Rete". Neologismo abbastanza usato derivato da network e citizen.

NEWBIE: Neologismo gergale che indica un nuovo utente della rete, un navigatore alle prime armi.

HOAX (FINTE MAIL): Un fenomeno legato al phishing e al furto di identità. Si tratta di finte mail, per esempio provenienti da istituti bancari o altri organismi, il cui unico scopo è sottrarre informazioni personali.

NICKNAME: Quando non si vuole usare il proprio nome in rete, si può scegliere un soprannome, detto appunto nickname. Non è possibile sapere chi si nasconde dietro a un nickname, per questo occorre fare molta attenzione quando si naviga in rete e ci si raffronta con altri utenti.

PEER- TO-PEER: Architettura di rete nella quale tutti i computer funzionano sia come client sia come server. Tutti i computer sono quindi uguali e di pari livello. Un esempio di rete peer-to-peer è Emule. Spesso questo tipo di reti vengono utilizzate per scambiare file illegalmente.

PHARMING: Tecnica che permette di sfruttare a proprio vantaggio le vulnerabilità di server controllando il dominio di un sito e utilizzandolo per ridirigere il traffico su altro sito.

PARENTAL CONTROL: Un filtro che permette di bloccare la visione dei contenuti non adatti ai bambini o a persone particolarmente sensibili

PHISHING: Il phishing è un furto di identità on line. Si basa su e-mail, notifiche esiti web fraudolenti progettati per rubare dati personali o informazioni riser*vate* come dati account, numeri di carte di

credito, password o altro.

POP-UP: Il termine significa "saltar su" e indica le finestre che si aprono nel browser in modo automatico, di solito a scopi pubblicitari.

PROXY SERVER: Un server che si interpone tra i computer di chi naviga e il Web. Il suo scopo è sia quello di incrementare le prestazioni di navigazione, verificando se la pagina richiesta è già disponibile in memoria, sia di filtrare la navigazione, per esempio per impedire ai dipendenti di visitare siti vietati o aree particolari.

RIPPER: Letteralmente "squartatore". È così definito un programma che acquisisce i dati da CD musicale a DVD *video* e li importa sul disco fisso, per un'eventuale conversione e modifica. Questo genere di azioni è quasi sempre illegale.

SPAM: Lo spam è qualsiasi tipo di comunicazione on line indesiderata. Attualmente la forma più comune di spam è la posta elettronica, per questo sono nate tecnologie, come il filtro SmartScreen di Microsoft, che riduce drasticamente la posta indesiderata in grado di raggiungere la nostra casella di posta.

SPYWARE: Spyware è un termine che descrive un software che si installa sul computer senza il tuo consenso. Uno spyware può fare pubblicità, raccogliere informazioni personali e addirittura arrivare a modificare la configurazione del tuo computer.

SSL: Acronimo di "Secure Sockets layer", un protocollo che rende sicure le transazioni commerciali in rete, per esempio con carte di credito, grazie alla trasmissione dei dati cifrata.

TRACKING PROTECTION LIST: La TPL o Protezione da monitoraggio, permette di scegliere i siti autorizzati a ricevere le informazioni che riguardano la navigazione da parte dell'utente e di controllare la propria privacy durante la navigazione.

TROJAN: È un software che nasconde al suo interno un virus. Installando ed eseguendo il programma che contiene il Trojan, l'utente innesca il virus.

VIRUS: I virus informatici sono software progettati per diffondersi da un computer all'altro e interferire con il funzionamento della macchina. Un virus può cancellare dati, carpire informazioni, usare il programma di posta per diffondersi ad altre macchine e addirittura rendere il PC inutilizzabile.

Warez: Neologismo usato per individuare software scaricabili abusivamente e illegalmente dalla rete.

WEP: Acronimo di Wired Equivalent Privacy, un sistema di crittografia che si basa su una chiave pubblica. Serve per rendere più sicure le comunicazioni wireless. Fa parte dei protocolli di sicurezza wireless anche l'algorismo di crittografia AES, sigla di Advance Encryption Standard.

WORM: Un worm è un particolare virus informatico in grado di propagarsi senza la necessità che l'utente inneschi il suo funzionamento compiendo un'operazione, per esempio installando un software.

Il Dirigente Scolastico
Calogero De Gregorio
Firma autografa sostituita a mezzo stampa
ai sensi dell'art. 3, comma 2 del D.Lg. 39/93