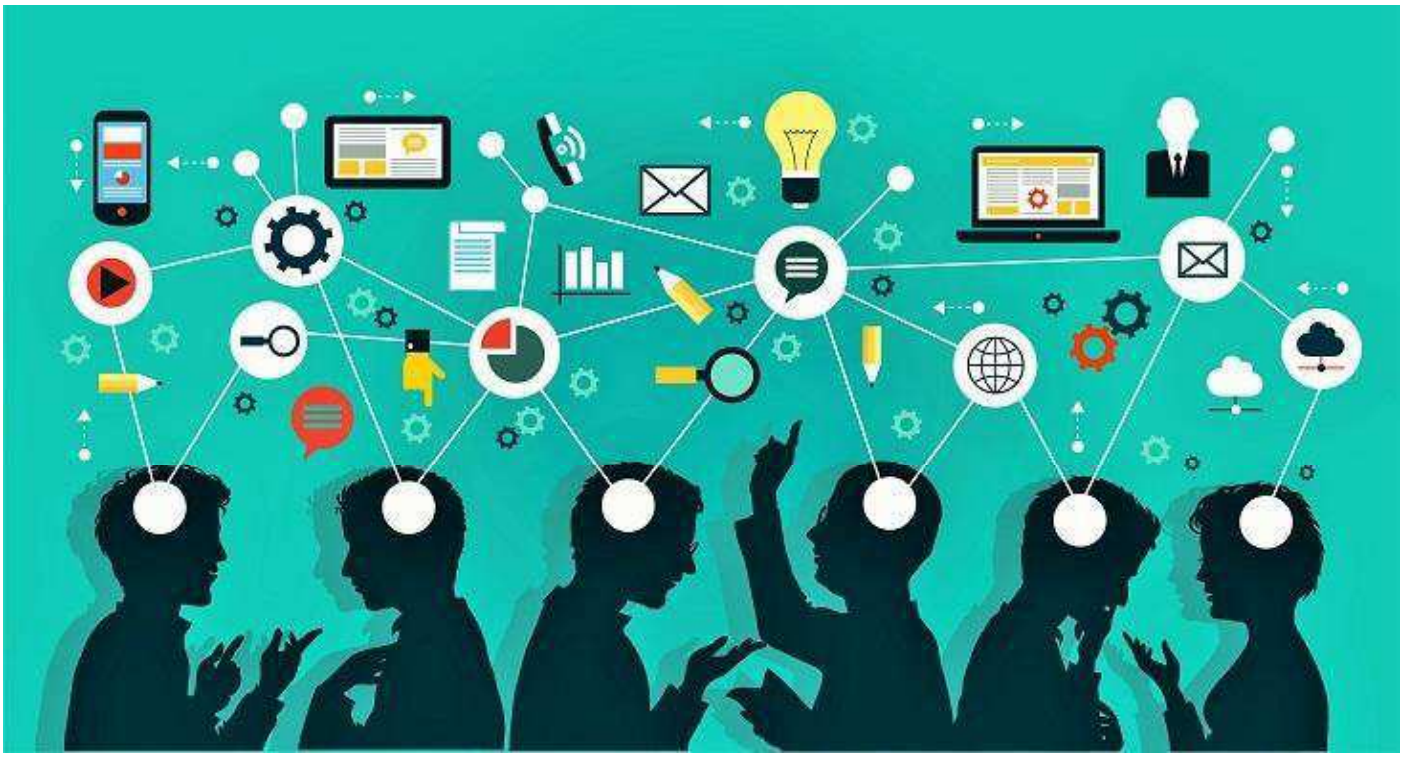
Istituto Scolastico Comprensivo Statale Igea

Scuola dell'Infanzia – Scuola Primaria – Scuola Secondaria di I Grado

Via Nicolò Zeno, 21 - 47814 BELLARIA IGEA MARINA (RN)

Codice Ministeriale: RNIC81500G Codice Fiscale: 91136840401 Codice Univoco Ufficio: UFMZDT

Tel. 0541/343980 - *Sito web:* https://www.icigeamarina.gov.it - *e-mail:* rnic81500g@istruzione.it - *P.E.C.:* rnic81500g@pec.istruzione.it - Fax 0541/343990



E-Safety Policy

a. s. 2017/2018

INDICE

1. INTRODUZIONE

1.1. Scopo della Policy

La creazione di una *E-Safety Policy,* da intendersi come una forma di regolamento d'istituto sull'utilizzo delle tecnologie digitali e della rete *Internet,* nasce dall'esigenza di stabilire norme precise, univoche, condivise e sottoscritte da tutti i soggetti coinvolti.

Tale documento si presenta come una risorsa per tutti i membri della comunità scolastica: una tutela per gli alunni che frequentano il nostro istituto, una guida per i docenti affinché possano operare in modo sicuro e responsabile, una garanzia per le famiglie che i propri figli possano apprendere e crescere in un ambiente sicuro e protetto dai numerosi rischi e dalle insidie in cui ogni giorno possono imbattersi utilizzando la rete *Internet.*

Attraverso la stesura di una *e-Policy* il nostro istituto comprensivo intende definire in modo trasparente e chiaro quali comportamenti siano da considerarsi leciti e quali illeciti, predisponendo per questi ultimi adeguati strumenti di prevenzione, controllo e monitoraggio, anche attraverso procedure precise di intervento e segnalazione.

Il regolamento vuole essere, dunque, uno strumento fruibile, di facile consultazione e applicazione per tutti gli operatori scolastici e per le famiglie, laddove è priorità e dovere della scuola garantire il benessere psicologico, sociale e formativo degli studenti.

1.2. Ruoli e responsabilità

Le informazioni e le indicazioni contenute in questo documento vogliono essere delle linee guida per un utilizzo corretto delle nuove tecnologie e della rete sia in ambiente scolastico sia extrascolastico; per questo motivo è molto importante che siano conosciute e condivise da tutte le figure che operano con i ragazzi a livello didattico ed educativo. E' auspicabile dunque che tali regole siano applicate sempre e non solo in ambito scolastico.

Di seguito si definiscono i ruoli e i compiti delle varie figure coinvolte:

RUOLO	COMPITI E RESPONSABILITA'
DOCENTI	➢ utilizzano nella propria azione didattica ed educativa le nuove tecnologie coerentemente con la propria programmazione e con il curricolo e i progetti esplicitati nel PTOF d'Istituto ➢ devono supervisionare e monitorare gli alunni quando utilizzano le strumentazioni tecnologiche ed internet nello svolgimento delle varie attività didattiche (sia in classe che in eventuali laboratori), in modo che non accedano a siti non autorizzati ➢ forniscono, in caso di ricerche assegnate autonomamente, adeguate sitografie ➢ istruiscono sulle modalità di utilizzo corretto della rete e sulle problematiche legate ad un uso improprio della stessa (legge sulla violazione della *privacy*, *copyright*, ecc….) ➢ mantengono segrete e custodite le proprie *password* e credenziali personali, non divulgandole a terzi ➢ conoscono e applicano scrupolosamente il regolamento del laboratorio di informatica

ALUNNI	➢ devono conoscere, accettare e sottoscrivere la *E-Safety Policy*, visionabile in formato digitale sul sito dell'istituto e in formato cartaceo negli uffici di segreteria ➢ non utilizzano a scuola telefono cellulare o altri dispositivi elettronici (*tablet*, *smartphone*, *I-pod*, registratori, macchine digitali, etc.), se non previa autorizzazione dei docenti ed esclusivamente a fini didattici ➢ utilizzano le TIC sempre col supporto e l'autorizzazione del docente e/o educatore presente ➢ conoscono le modalità di utilizzo corretto della rete e delle problematiche legate ad un uso improprio della stessa (legge sulla violazione della *privacy*, *copyright*, ecc….) ➢ usano adeguatamente ed in modo responsabile le strumentazioni a disposizione (pc, chiavette usb, cd-rom, dvd o altri dispositivi esterni di proprietà della scuola o propri) sotto la supervisione dei docenti ➢ segnalano a figure adulte (genitori, docenti, personale scolastico, …) eventuali comportamenti scorretti, pericolosi o inadeguati da parte propria o di altri ➢ mantengono segrete e custodite le proprie *password* e credenziali personali e/o familiari, non divulgandole a terzi ➢ non devono installare su dispositivi scolastici software e ogni altra applicazione ➢ possono acquisire foto e video durante l'orario scolastico solo previa autorizzazione dei docenti ➢ non possono mettere in rete o condividere fotografie, video personali o di terzi ➢ non utilizzano i dispositivi tecnologici per giochi, ascolto di musica o altro, non pertinente con l'attività didattica ➢ archiviano i propri *file* correttamente secondo le istruzioni fornite dai docenti e chiudono sempre correttamente la sessione di lavoro ➢ si confrontano con gli adulti in caso di dubbi ed incertezze sui comportamenti più appropriati da tenere in relazione all'uso delle TIC
GENITORI/TUTORI	➢ devono conoscere, accettare e sottoscrivere la *E-Safety policy* ➢ mantengono segrete e custodite le proprie *password* e credenziali personali e/o familiari , non divulgandole a terzi ➢ segnalano tempestivamente ai docenti coordinatori eventuali sospetti di un utilizzo non consono dei *device* (strumenti digitali) da parte dei propri figli o altri alunni durante l'attività scolastica ➢ accettano e sottoscrivono la Dichiarazione liberatoria per la pubblicazione di elaborati, video, foto, presente sul diario di istituto
DIRIGENTE	➢ Approva la E-Safety policy e ne è responsabile in quanto rappresentante dell'intera comunità scolastica ➢ raccoglie segnalazioni da parte dei docenti e del personale scolastico di comportamenti inappropriati e non conformi al regolamento ➢ interviene in casi di violazione o non rispetto delle regole stabilite da parte di docenti, personale scolastico e/o alunni ➢ garantisce che la scuola utilizzi filtri sicuri per l'accesso a internet, conformi alla normativa vigente

1.3. Condivisione e comunicazione della *Policy* all'intera comunità scolastica

La *E-Safety Policy* è pubblicata e consultabile sul sito della scuola www.icigeamarina.gov.it, esposta all'Albo d'Istituto e nei diversi plessi. Tutta la comunità scolastica è tenuta a prenderne visione, mentre è compito dei docenti illustrare agli alunni in modo adeguato alla loro età il contenuto della stessa, sottolineando in particolare i rischi di un uso improprio delle strumentazioni e della rete, educandoli al senso di responsabilità personale.

1.4. Gestione delle infrazioni alla *Policy*

Nel caso in cui le norme presenti all'interno di questo documento vengano violate e/o si riscontrino dei danneggiamenti ai vari strumenti posti a disposizione dalla scuola, l'istituzione scolastica adotterà sanzioni disciplinari rapportate alla gravità degli episodi e alle fasce d'età degli studenti coinvolti.

Le violazioni continue e/o ripetute delle presenti normative potranno comportare dei provvedimenti di natura didattica e/o disciplinare stabiliti dai docenti del Consiglio di classe, ma anche il divieto temporaneo o, nei casi più gravi, permanente, di accesso alle risorse informatiche e alla rete.

Qualora le infrazioni si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. Infatti è bene ricordare a tutti che nel momento in cui un qualunque attore della comunità scolastica (Dirigente, docente, personale ATA, …) venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia (ex art. 331 del codice di procedura penale). L'omissione di denuncia costituisce reato (art. 361). I reati che, in ambiente scolastico, possono essere riferiti all'ambito digitale e commessi per via telematica sono tra gli altri:

- ✓ minaccia, in particolare, se la minaccia è grave, per tale reato si procede d'ufficio (art. 612 codice penale);
- ✓ induzione alla prostituzione minorile (art. 600bis);
- ✓ pedopornografia (art. 600ter);
- ✓ corruzione di minorenne (art. 609 quinquies).
- ✓ lesione della reputazione digitale (art 595) (Corte di Cassazione, sez. V penale, sentenza n. 4873/2017).

Nel caso in cui le infrazioni della policy violino norme previste dal Regolamento di Istituto si procede secondo quanto previsto dal Regolamento stesso. La violazione o il dolo accertato, oltre a sanzioni disciplinari stabiliti dal Consiglio di Classe, potrebbero comportare la richiesta di un risarcimento nella misura del danno provocato e comunque decisa dal Dirigente Scolastico, in uno spirito di recupero e rieducazione.

1.5. Monitoraggio dell'implementazione della *Policy* e suo aggiornamento

Questo documento verrà revisionato periodicamente e, se necessario, verranno messe in atto tutte le azioni migliorative che il Collegio dei Docenti riterrà opportuno attuare al fine di rendere la E-Safety Policy sempre più parte viva ed integrante del Regolamento e del PTOF d'Istituto.

1.6. Integrazione della *Policy* con regolamenti esistenti

Tale documento è parte integrante del Regolamento d'Istituto ed è approvato e ratificato dal Collegio Docenti e dal Consiglio d'Istituto. E' sottoscritto dai genitori/tutori a inizio dell'anno scolastico e può essere oggetto di revisione periodica.

La P*olicy* richiede l'integrazione con l'inserimento delle seguenti norme:

REGOLAMENTO SULL'UTILIZZO DEL LABORATORIO DI INFORMATICA, DELLE POSTAZIONI DI LAVORO E DELL'UTILIZZO DI INTERNET "I.C. Igea Scuola Secondaria di I grado"

Disposizioni sull'uso del laboratorio:

PREMESSA GENERALE

Le nuove tecnologie informatiche rappresentano per la scuola un importante strumento per rinnovare ed ampliare le possibilità didattiche e la ricerca culturale.

Pertanto gli Istituti Comprensivi Bellaria e Igea intendono incrementare l'uso di queste risorse creando attorno alle risorse informatiche comuni della scuola un clima di "condivisione" e di "corresponsabilità", che coinvolga tutti gli utenti in una cogestione convinta delle regole di accesso e di funzionamento, in modo che ciascuno contribuisca a rispettare e a far rispettare il presente regolamento.

Il laboratorio d'informatica della scuola secondaria di primo grado è patrimonio comune, pertanto si ricorda che il rispetto e la tutela delle attrezzature sono condizioni indispensabili per il loro utilizzo e per mantenere l'efficienza del laboratorio stesso.

Definire all'interno dell'Istituzione scolastica regole chiare è una buona base per lavorare serenamente, sicuri di aver posto in atto quanto possibile in chiave di prevenzione. A tal fine si stila un regolamento per l'utilizzo e il corretto funzionamento delle aule e delle postazioni informatiche, tramite l'indicazione di prassi opportune e l'invito a un uso sempre più professionale da parte di tutto il personale.

L'osservazione di norme di buona educazione e un corretto comportamento permettono un adeguato funzionamento dello svolgimento delle attività presso il laboratorio e preservano le attrezzature, i materiali e le tecnologie di cui si dispone.

È compito dei docenti far osservare e rispettare il regolamento di ciascun laboratorio. Atti di vandalismo verranno perseguiti nelle forme previste, compreso il risarcimento degli eventuali danni arrecati.

Il presente Regolamento richiama la responsabilità del personale interessato sull'osservanza di alcune fondamentali regole di comportamento in ordine al corretto utilizzo degli strumenti di laboratorio al fine di preservarne la piena funzionalità.

L'accesso al laboratorio d'informatica è subordinato all'accettazione del presente regolamento tramite firma su apposito modulo.

I docenti si impegnano a spiegare e a far rispettare le norme di seguito elencate.

La mancata sorveglianza di alunni o del rispetto di questo regolamento comporta la corresponsabilità su eventuali danni o disfunzioni.

Per l'anno scolastico 2015-2016 il responsabile del laboratorio d'informatica è il Prof. Fabio Moretti.

Il Responsabile del Laboratorio fornisce la consulenza necessaria:

- sulla disponibilità e le caratteristiche generali dei mezzi e dei programmi in dotazione;
- sull'uso corretto ed efficiente delle attrezzature del Laboratorio;
- sulle tecniche di utilizzo dei sistemi e delle risorse di rete;
- coordina l'attività col personale tecnico.

Norme da seguire durante il trasferimento della classe al laboratorio

Durante il percorso per raggiungere il laboratorio, gli alunni dovranno tenere un comportamento adeguato:

- non saranno minimamente tollerati atti di prevaricazione e di violenza verso gli altri;
- non correre per il corridoio e non spingere;
- tenere un tono di voce normale e non gridare;
- usare un linguaggio rispettoso e corretto;
- non spostarsi senza autorizzazione e sempre sotto la guida del docente accompagnatore;
- procedere in modo ordinato (in fila) e silenzioso, eventualmente chiacchierando a voce bassa;
- mantenere puliti e in ordine gli spazi scolastici ed usare con cura il materiale e gli arredi;
- mantenere, fino alla fine della lezione, il comportamento corretto ed educato.

Al fine di ottimizzare l'uso del laboratorio, si comunica che l'accesso ad esso è regolato dalle seguenti norme:

Art. 1. L'accesso al laboratorio d'informatica è riservato ai docenti e gli alunni degli Istituti Comprensivi "Bellaria" e "Igea", altre persone presenti a vario titolo nella scuola devono concordare l'eventuale uso del laboratorio con il dirigente scolastico e con il responsabile dell'aula;

Art. 2. Ai laboratori si accede solo per ragioni inerenti l'attività scolastica, sia di tipo strettamente didattico (ore curricolari di laboratorio, attività didattiche integrative e di recupero, progetti approvati dal POF, preparazione di tesine e ricerche didattiche) e di organizzazione del lavoro individuale del docente (piani di lavoro, progetti, autoaggiornamento, altre attività accessorie l'insegnamento della propria materia). Non è consentito ad altri insegnanti l'accesso ai laboratori per usufruire di una postazione libera mentre è in corso una lezione di un altro collega, a meno che questi non acconsenta esplicitamente;

Art. 3. L'accesso al laboratorio avviene previa prenotazione su apposito "REGISTRO DELLE PRENOTAZIONI", l'orario in cui l'aula è occupata viene affisso nei pressi dell'aula;

Art. 4. L'accesso agli alunni è consentito solo in presenza di un docente e non possono mai, in nessun caso, restare da soli nell'aula d'informatica;
Art. 5. Gli utenti che a qualunque titolo utilizzano l'aula dovranno obbligatoriamente compilare dettagliatamente e in ogni parte il "REGISTRO DELLE PRESENZE" indicando l'orario di ingresso, quello d'uscita e la motivazione dell'uso delle postazioni informatiche. Questo allo scopo di poter risalire alle cause di eventuali inconvenienti o danneggiamenti e per comprovare l'effettivo utilizzo dell'aula;
Art. 6. Se non si usa l'aula nei giorni che erano comunque stati assegnati, darne comunicazione al responsabile affinché possano usufruirne altre classi;
Art. 7. E' vietato l'accesso all'aula in maniera estemporanea e improvvisata. Nei giorni e negli orari nei quali l'uso dell'aula non è stato assegnato ad alcuna classe, è possibile prenotarne l'uso contattando il responsabile dell'aula d'informatica con almeno un giorno d'anticipo;
Art. 8. Ogni docente è tenuto ad aprire e chiudere l'aula mediante richiesta diretta e riconsegna delle chiavi ai collaboratori scolastici. Non è ammessa la consegna delle chiavi agli alunni.
Art. 9. Ogni utente è tenuto a procedere all'accensione delle attrezzature e all'iniziale ricognizione dell'integrità delle stesse, tale verifica dovrà essere fatta anche al termine della loro attività;
Art. 10. Il docente accompagnatore deve assegnare a ciascun alunno una POSTAZIONE PERMANENTE;
Art. 11. E' assolutamente vietato scrivere sui banchi, monitor, mouse, tastiere o altro;
Art. 12. E' assolutamente vietato toccare con le dita i monitor;
Art. 13. Curarsi di usare le attrezzature con le mani pulite;
Art. 14. Il docente accompagnatore durante l'ora a sua disposizione per lezioni o esercitazioni osserverà la massima vigilanza sul comportamento degli alunni e sul rispetto degli stessi per il materiale informatico e per le attrezzature in dotazione dell'aula e deve accertarsi che gli alunni assumano sempre una postura corretta davanti al pc;
Art. 15. È vietato aprire, manomettere in qualsiasi modo o asportare le suppellettili e le apparecchiature dal laboratorio, nonché utilizzare attrezzature laddove le stesse non siano necessarie per il tipo di utilizzo fatto;
Art. 16. È severamente vietato staccare cavi elettrici da ciabatte e prese così come i cavi di connessione alle periferiche;
Art. 17. È vietato modificare in alcun modo l'hardware e il software di sistema. Non è consentita l'installazione di nuovi programmi software o altro hardware che è di esclusiva competenza dell'amministratore dei sistemi. I docenti che hanno necessità di installare programmi o cd-rom sono pregati di contattare i responsabili del laboratorio per avere le indicazioni necessarie;
Art. 18. Non modificare le impostazioni (salvaschermo, sfondo, colori, risoluzioni, suoni, ecc.);
Art. 19. Non modificare o inserire nessun tipo di password;
Art. 20. E' vietato cancellare o alterare file - dati presenti in *hard-disk*; in particolare è assolutamente vietato aprire, spostare o eliminare dati e cartelle altrui;
Art. 21. I propri file vanno memorizzati nella cartella *Documenti condivisi,*creando una propria cartella personale nella quale *memorizzare i dati in modo ordinato*; all'interno della cartella di ogni docente si crea una cartella per ogni classe dentro cui si crea una cartella per ogni alunno della classe. I vari lavori creati o i file scaricati andranno salvati da alunni e docenti nella propria cartella (non nel desktop da dove verranno cancellati automaticamente ad ogni riavvio);
Art. 22. Se dovessero servire programmi specifici si farà richiesta alla funzione strumentale che valuterà l'opportunità dell'acquisto, fermo restando la disponibilità di fondi e privilegiando comunque l'uso di software *opensource*.
Art. 23. Non si assume alcuna responsabilità per la perdita o cancellazione di dati personali, si raccomanda pertanto vivamente di salvare i propri dati nella cartella indicata dall'insegnante o su un supporto esterno, ad esempio una *pen-drive*;
Art. 24. Occorre chiudere correttamente qualsiasi programma utilizzato prima di spegnere il computer;
Art. 25. Occorre spegnere i computer utilizzando sempre la procedura corretta;
Art. 26. Nell'aula è vietato mangiare, bere, ed in generale svolgere la ricreazione;
Art. 27. Nell'aula è assolutamente vietato spostarsi da una postazione all'altra;
Art. 28. E' assolutamente vietato far entrare nel laboratorio persone non autorizzate;
Art. 29. Nell'aula non è consentito il deposito di zaini e cappotti.
Art. 30. Eventuali danni, manomissioni, danneggiamenti o furti dovranno essere tempestivamente segnalati dagli utenti (verbalmente o mediante registro) al responsabile del laboratorio o al Dirigente Scolastico.

ACCESSO AD INTERNET
Art. 31. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante che segue gli alunni in tutte le fasi della navigazione;
Art. 32. Internet non può essere usato per scopi vietati dalla legislazione vigente;
Art. 33. Non permettere agli alunni di inoltrare dati personali tramite mail (nome, cognome, indirizzo);
Art. 34. Non aprire file con allegati provenienti da mittenti sconosciuti (potrebbero contenere virus!);
Art. 35. Copiando materiale da Internet, tener presente delle leggi sui diritti d'autore e di proprietà intellettuale;
Art. 36. Laddove ci siano alunni che effettuano accessi a siti che non hanno alcuna valenza didattica e di contenuto diseducativo, il docente ha l'obbligo di ammonire la prima volta verbalmente poi invece per iscritto tali alunni sul registro di classe, ed interrompere l'attività che prevede il collegamento ad Internet;
Art. 37. Non è possibile utilizzare applicazioni di messaggistica istantanea (*chat* e *sms*), *social network* (*facebook*, *Twitter*, ecc) o

posta elettronica per uso personale;
Art. 38. Non è consentito giocare online almeno che non sia il docente a specificare l'indirizzo e il gioco prescelto per uso didattico;
Art. 39. Gli utenti sono informati che tutto ciò che viene fatto su ciascuna delle nostre macchine è debitamente registrato, cosa che rende possibili controlli molto accurati;

UTILIZZO DELLA STAMPANTE
Art. 40. La sostituzione delle cartucce delle stampanti è di competenza dei responsabili di laboratorio;
Art. 41. Limitare l'uso delle stampanti all'effettiva necessità di lavoro ed evitarne l'uso a titolo personale;
Art. 42. Prima di stampare utilizzare la funzione *Anteprima di Stampa* al fine di annullare eventuali stampe inutili, ripetute o errate;
Art. 43. Evitare code di stampa cliccando svariate volte sul comando "Stampa";
Art. 44. Indicare sul registro delle presenze il numero di stampe fatte;

QUANDO SI LASCIA IL LABORATORIO
Art. 45. Al termine della sessione di lavoro l'utente è tenuto a lasciare la postazione di lavoro pulita e in ordine (risistemare tastiere, schermi, mouse, sedie e quant'altro come sono stati trovati all'ingresso) non dimenticare floppy disk, pen drive, cd rom...;
Art. 46. Accertarsi che tutti i PC, il videoproiettore e le casse acustiche e le stampanti siano spenti; in caso di malfunzionamenti comunicarlo immediatamente al responsabile.
Art. 47. Non toccare il quadro elettrico generale;
Art. 48. Chiudere a chiave il laboratorio le chiavi dell'aula, al termine delle lezioni, devono essere sempre riconsegnate al personale ausiliario;

CESSIONE DELL'USO DEI LABORATORI A TERZE PARTI
Nel caso in cui i laboratori vengano concessi in utilizzo a enti esterni per scopi extracurriculari (corsi di aggiornamento, concorsi, attività pomeridiane in genere), il Dirigente Scolastico concorderà l'attività con il consegnatario dei beni, e il responsabile del laboratorio. Questi provvederà ad avvisare tempestivamente i colleghi della cessione. I tutor o responsabili di tali corsi sono tenuti a prendere contatto con il Responsabile del laboratorio per prendere visione della dotazione dei laboratori e del regolamento e per convenire eventuali modalità di utilizzo.
Nella concessione dei laboratori si dovrà comunque tenere conto della disponibilità dei laboratori stessi e della priorità di necessità didattiche evidenziate dagli insegnanti dell'Istituto.

REGOLAMENTO PER ACCESSO DA PARTE DI ESTERNI
Art. 49. Chiunque acceda al laboratorio a qualunque titolo è vincolato dal rispetto del seguente regolamento, pena l'interdizione dell'uso del laboratorio.
Art. 50. Ogni ente esterno dovrà contattare per tempo il responsabile del laboratorio di informatica per concordare il programma, le applicazioni, i programmi necessari e le risorse di rete utili.
Art. 51. Ogni utente esterno alla scuola deve e compilare il modulo presenze per intero e firmare il modulo per il trattamento dei dati sensibili.
Art. 52. I Tutor e i responsabili dei corsi esterni devono vigilare sul rispetto del regolamento da parte dei partecipanti.

NORME FINALI
I Responsabili di laboratorio che verifichino un uso del laboratorio contrario a disposizioni di legge o del regolamento interno, ne danno comunicazione al Dirigente Scolastico che provvederà ai dovuti provvedimenti e in casi gravi a interrompere l'ingresso nell'aula di informatica.
I responsabili del laboratori sono a disposizione per qualsiasi esigenza di supporto.
Il presente regolamento deve essere *stampato*, *illustrato* ai docenti di tutte le scuole dell'istituto e *affisso* nel laboratorio d'informatica

REGOLAMENTO DEL LABORATORIO DI INFORMATICA DELLA SCUOLA PRIMARIA "A. Ferrarin"

SEZ. 1. CHI PUÒ ACCEDERE AL LABORATORIO E PRENOTAZIONE
Art. 1. L'accesso al laboratorio d'informatica è riservato ai docenti e gli alunni della scuola Primaria "A. Ferrarin" dell'Istituto Comprensivo Igea, altre persone presenti a vario titolo nella scuola devono concordare l'eventuale uso del laboratorio con il dirigente scolastico e con il responsabile dell'aula ;
Art. 2. Ai laboratori si accede solo per ragioni inerenti l'attività scolastica, sia di tipo strettamente didattico che di organizzazione del lavoro individuale del docente. Non è consentito ad altri insegnanti l'accesso ai laboratori per usufruire di una postazione libera mentre è in corso una lezione di un altro collega, a meno che questi non acconsenta esplicitamente;

Art. 3. L'accesso agli alunni è consentito solo in presenza di un docente e non possono mai, in nessun caso, restare da soli nell'aula d'informatica;
Art. 4. E' assolutamente vietato l'accesso al laboratorio di persone non autorizzate;

SEZ. 2. PRASSI DI ACCESSO AL LABORATORIO E COMPORTAMENTI DA TENERE ALL'INTERNO
Art. 5. Ogni docente è tenuto ad aprire e chiudere l'aula mediante richiesta diretta e riconsegna delle chiavi ai collaboratori scolastici o al responsabile del laboratorio. Non è ammessa la consegna delle chiavi agli alunni.
Art. 6. Il docente accompagnatore durante l'ora a sua disposizione per lezioni o esercitazioni osserverà la massima vigilanza sul comportamento degli alunni e sul rispetto degli stessi per il materiale informatico e per le attrezzature in dotazione dell'aula e deve accertarsi che gli alunni assumano sempre una postura corretta davanti al pc;
Art. 7. Ogni insegnante è responsabile di istruire i propri alunni nelle procedure di accensione, spegnimento e utilizzo del computer;
Art.8. Ogni utente è tenuto a procedere all'accensione delle attrezzature e all'iniziale ricognizione dell'integrità delle stesse, tale verifica dovrà essere fatta anche al termine della loro attività;
Art. 9. E' assolutamente vietato scrivere sui banchi, monitor, mouse, tastiere o altro;
Art. 10. Curarsi di usare le attrezzature con le mani pulite;
Art. 11. È vietato aprire, manomettere in qualsiasi modo o asportare le suppellettili e le apparecchiature dal laboratorio (mouse, tastiere, stampanti, casse, ecc. …);
Art. 12. È vietato staccare cavi elettrici da ciabatte e prese così come i cavi di connessione alle periferiche;
Art. 13. Non modificare le impostazioni (salvaschermo, sfondo, colori, risoluzioni, suoni, ecc.);
Art. 14. Nell'aula è vietato mangiare, bere ed in generale svolgere la ricreazione.

SEZ. 3. USO DI STRUMENTI DI MASSA E FILE ESTRANEI
Art. 15. Non modificare o inserire nessun tipo di password; e' vietato cancellare o alterare file - dati presenti in hard-disk; in particolare è assolutamente vietato aprire, spostare o eliminare dati e cartelle altrui; questo può essere fatto solo dal responsabile qualora si renda necessario;
Art. 16. È vietato modificare in alcun modo l'hardware e il software di sistema. Non è consentita l'installazione di nuovi programmi software o altro hardware che è di esclusiva competenza del responsabile del laboratorio o dell'animatore digitale. I docenti che hanno necessità di installare programmi o cd-rom sono pregati di contattare il responsabile del laboratorio per avere le indicazioni necessarie;
Art. 17. I propri file vanno memorizzati all'interno di una cartella personale o di classe che ogni docente deve crearsi e dentro cui ogni alunno può salvare il proprio lavoro in modo ordinato. La cartella va salvata su **"COLLEGAMENTO FERRARIN"**presente sul desktop;
Art. 18. Non si assume alcuna responsabilità per la perdita o cancellazione di dati personali, si raccomanda pertanto vivamente di salvare i propri dati nella cartella indicata dall'insegnante o su un supporto esterno, ad esempio una pen-drive;
Art. 19. In caso si volesse utilizzare una pen-drive si dovrà eseguire una scansione antivirus prima di aprire la cartella file;
Art. 20. In caso si dovesse utilizzare un file .zip o archivio zippato in genere si dovrà, prima di aprire il file, cliccare con il tasto destro del mouse e avviare una scansione antivirus;
Art. 21. Occorre chiudere correttamente qualsiasi programma utilizzato prima di spegnere il computer;
Art. 22. Ogni giorno un docente incaricato si preoccuperà di spegnere i computers utilizzando sempre la procedura corretta. In caso il computer segnalasse l'installazione di aggiornamenti si spegnerà il monitor senza forzare lo spegnimento del computer;
Art. 23. Eventuali danni, manomissioni, danneggiamenti o furti dovranno essere tempestivamente segnalati dagli utenti (verbalmente e mediante mail) al responsabile del laboratorio e al animatore digitale.

SEZ. 4. ACCESSO AD INTERNET
Art. 24. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante che segue gli alunni in tutte le fasi della navigazione;
Art. 25. Internet non può essere usato per scopi vietati dalla legislazione vigente;
Art. 26. Non permettere agli alunni di inoltrare dati personali tramite mail (nome, cognome, indirizzo);
Art. 27. Non aprire file con allegati provenienti da mittenti sconosciuti (potrebbero contenere virus!);
Art. 28. Copiando materiale da Internet, tener presente le leggi sui diritti d'autore e di proprietà intellettuale;
Art. 29. Laddove ci siano alunni che effettuano accessi a siti che non hanno alcuna valenza didattica e di contenuto diseducativo, il docente ha l'obbligo di ammonire ed interrompere l'attività che prevede il collegamento ad Internet;
Art. 30. Non è possibile utilizzare applicazioni di messaggistica istantanea (chat e sms), social network (facebook, Twitter, ecc) o posta elettronica per uso personale;
Art. 31. Non è consentito giocare online almeno che non sia il docente a specificare l'indirizzo e il gioco prescelto per uso didattico;
Art. 32. Gli utenti sono informati che tutto ciò che viene fatto su ciascuna delle nostre macchine è debitamente registrato, cosa che rende possibili controlli molto accurati;

SEZ. 5. QUANDO SI LASCIA IL LABORATORIO

Art. 33. Al termine della sessione di lavoro l'utente è tenuto a lasciare la postazione di lavoro pulita e in ordine (risistemare tastiere, schermi, mouse, sedie e quant'altro come sono stati trovati all'ingresso)

Art. 34. Non toccare il quadro elettrico generale;

SEZ. 6. UTILIZZO DELLA STAMPANTE

Art. 35. La sostituzione delle cartucce delle stampanti è di competenza dei responsabili di laboratorio;

Art. 36. Limitare l'uso delle stampanti all'effettiva necessità di lavoro ed evitarne l'uso a titolo personale o sostituibile con l'uso della fotocopiatrice;

Art. 37. Prima di stampare utilizzare la funzione Anteprima di Stampa al fine di annullare eventuali stampe inutili, ripetute o errate;

Art. 38. Evitare code di stampa cliccando svariate volte sul comando "Stampa".

REGOLAMENTO DEL LABORATORIO DI INFORMATICA DELLA SCUOLA PRIMARIA " A. Manzi"

SEZ. 1. CHI PUÒ ACCEDERE AL LABORATORIO E PRENOTAZIONE

Art. 1. L'accesso al laboratorio d'informatica è riservato ai docenti e gli alunni della scuola Primaria "A. Manzi" dell'Istituto Comprensivo Igea, altre persone presenti a vario titolo nella scuola devono concordare l'eventuale uso del laboratorio con il dirigente scolastico e con il responsabile dell'aula;

Art. 2. Ai laboratori si accede solo per ragioni inerenti l'attività scolastica, sia di tipo strettamente didattico e di organizzazione del lavoro individuale del docente. Non è consentito ad altri insegnanti l'accesso ai laboratori per usufruire di una postazione libera mentre è in corso una lezione di un altro collega, a meno che questi non acconsenta esplicitamente;

Art. 3. L'accesso al laboratorio avviene previa prenotazione su apposito "REGISTRO DELLE PRENOTAZIONI", affisso alla porta che da accesso al corridoio del secondo piano che porta all'aula;

Art. 4. L'accesso agli alunni è consentito solo in presenza di un docente e non possono mai, in nessun caso, restare da soli nell'aula d'informatica;

Art. 5. Gli utenti che a qualunque titolo utilizzano l'aula dovranno obbligatoriamente compilare dettagliatamente e in ogni parte il "REGISTRO DELLE PRESENZE" indicando l'orario di ingresso, quello d'uscita e la motivazione dell'uso delle postazioni informatiche. Questo allo scopo di poter risalire alle cause di eventuali inconvenienti o danneggiamenti e per comprovare l'effettivo utilizzo dell'aula;

Art. 6. E' assolutamente vietato l'accesso al laboratorio di persone non autorizzate;

SEZ. 2. PRASSI DI ACCESSO AL LABORATORIO E COMPORTAMENTI DA TENERE ALL'INTERNO

Art. 7. Ogni docente è tenuto ad aprire e chiudere l'aula mediante richiesta diretta e riconsegna delle chiavi ai collaboratori scolastici o al responsabile del laboratorio. Non è ammessa la consegna delle chiavi agli alunni.

Art. 8. Il docente accompagnatore durante l'ora a sua disposizione per lezioni o esercitazioni osserverà la massima vigilanza sul comportamento degli alunni e sul rispetto degli stessi per il materiale informatico e per le attrezzature in dotazione dell'aula e deve accertarsi che gli alunni assumano sempre una postura corretta davanti al pc;

Art. 9. Ogni insegnante è responsabile di istruire i propri alunni nelle procedure di accensione, spegnimento e utilizzo del computer;

Art. 10. Ogni utente è tenuto a procedere all'accensione delle attrezzature e all'iniziale ricognizione dell'integrità delle stesse, tale verifica dovrà essere fatta anche al termine della loro attività;

Art. 11. E' assolutamente vietato scrivere sui banchi, monitor, mouse, tastiere o altro;

Art. 12. E' assolutamente vietato toccare con le dita i monitor;

Art. 13. Curarsi di usare le attrezzature con le mani pulite;

Art. 14. È vietato aprire, manomettere in qualsiasi modo o asportare le suppellettili e le apparecchiature dal laboratorio (mouse, tastiere, stampanti, casse, ecc. …);

Art. 15. È severamente vietato staccare cavi elettrici da ciabatte e prese così come i cavi di connessione alle periferiche;

Art. 16. Non modificare le impostazioni (salvaschermo, sfondo, colori, risoluzioni, suoni, ecc.);

Art. 17. Nell'aula è vietato mangiare, bere ed in generale svolgere la ricreazione.

SEZ. 3. USO DI STRUMENTI DI MASSA E FILE ESTRANEI

Art. 18. Non modificare o inserire nessun tipo di password; E' vietato cancellare o alterare file - dati presenti in hard-disk; in particolare è assolutamente vietato aprire, spostare o eliminare dati e cartelle altrui;

Art. 19. È vietato modificare in alcun modo l'hardware e il software di sistema. Non è consentita l'installazione di nuovi programmi software o altro hardware che è di esclusiva competenza del responsabile del laboratorio o dell'animatore digitale. I docenti che hanno necessità di installare programmi o cd-rom sono pregati di contattare il responsabile del laboratorio per avere le indicazioni necessarie;

Art. 20. I propri file vanno memorizzati nella cartella USER presente sul desktop , all'interno della cartella di ogni docente si crea una cartella per la classe dentro cui si ogni alunno può salvare il proprio lavoro in modo ordinato. I vari lavori creati o i file scaricati andranno salvati da alunni e docenti nella propria cartella (non nel desktop da dove verranno cancellati ogni volta che verrà eseguita una pulizia periodica);

Art. 21. Non si assume alcuna responsabilità per la perdita o cancellazione di dati personali, si raccomanda pertanto vivamente di salvare i propri dati nella cartella indicata dall'insegnante o su un supporto esterno, ad esempio una pen-drive;

Art. 22. In caso si volesse utilizzare una pen-drive si dovrà eseguire una scansione antivirus prima di aprire la cartella file;

Art. 23. In caso si dovesse utilizzare un file .zip o archivio zippato in genere si dovrà prima di aprire il file cliccare con il tasto destro del mouse e avviare una scansione antivirus;

Art. 24. Occorre chiudere correttamente qualsiasi programma utilizzato prima di spegnere il computer;

Art. 25. Occorre spegnere i computer utilizzando sempre la procedura corretta. In caso il computer segnalasse l'installazione di aggiornamenti si spegnerà il monitor senza forzare lo spegnimento del computer;

Art. 26. Eventuali danni, manomissioni, danneggiamenti o furti dovranno essere tempestivamente segnalati dagli utenti (verbalmente e mediante mail) al responsabile del laboratorio e al animatore digitale.

SEZ. 4. ACCESSO AD INTERNET

Art. 27. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante che segue gli alunni in tutte le fasi della navigazione;

Art. 28. Internet non può essere usato per scopi vietati dalla legislazione vigente;

Art. 29. Non permettere agli alunni di inoltrare dati personali tramite mail (nome, cognome, indirizzo);

Art. 30. Non aprire file con allegati provenienti da mittenti sconosciuti (potrebbero contenere virus!);

Art. 31. Copiando materiale da Internet, tener presente delle leggi sui diritti d'autore e di proprietà intellettuale;

Art. 32. Laddove ci siano alunni che effettuano accessi a siti che non hanno alcuna valenza didattica e di contenuto diseducativo, il docente ha l'obbligo di ammonire la prima volta verbalmente poi invece per iscritto tali alunni sul registro di classe, ed interrompere l'attività che prevede il collegamento ad Internet;

Art. 33. Non è possibile utilizzare applicazioni di messaggistica istantanea (chat e sms), social network (facebook, Twiter, ecc) o posta elettronica per uso personale;

Art. 34. Non è consentito giocare online almeno che non sia il docente a specificare l'indirizzo e il gioco prescelto per uso didattico;

Art. 35. Gli utenti sono informati che tutto ciò che viene fatto su ciascuna delle nostre macchine è debitamente registrato, cosa che rende possibili controlli molto accurati;

SEZ. 5. QUANDO SI LASCIA IL LABORATORIO

Art. 36. Al termine della sessione di lavoro l'utente è tenuto a lasciare la postazione di lavoro pulita e in ordine (risistemare tastiere, schermi, mouse, sedie e quant'altro come sono stati trovati all'ingresso) non dimenticare pen-drive, cd rom, quaderni, ecc.;

Art. 37. Accertarsi che tutti i PC, i monitor e le casse acustiche e la stampante siano spenti; in caso di malfunzionamenti comunicarlo immediatamente al responsabile del laboratorio e segnalarlo sul "REGISTRO PRESENZE";

Art. 38. Non toccare il quadro elettrico generale;

Art. 39. Chiudere a chiave il laboratorio le chiavi dell'aula, al termine delle lezioni, devono essere sempre riconsegnate al personale ausiliario o al responsabile del laboratorio;

SEZ. 6. UTILIZZO DELLA STAMPANTE

Art. 40. La sostituzione delle cartucce delle stampanti è di competenza deiresponsabili di laboratorio;

Art. 41. Limitare l'uso delle stampanti all'effettiva necessità di lavoro ed evitarne l'uso a titolo personale o sostituibile con l'uso della fotocopiatrice;

Art. 42. Prima di stampare utilizzare la funzione Anteprima di Stampa al fine di annullare eventuali stampe inutili, ripetute o errate;
Art. 43. Evitare code di stampa cliccando svariate volte sul comando "Stampa";
Art. 44. Indicare sul "REGISTRO STAMPANTE" il numero di stampe fatte.

Regolamento d'Istituto - UTILIZZO DEL TELEFONO CELLULARE E DEI VARI DISPOSITIVI ELETTRONICI DURANTE LE ATTIVITA' SCOLASTICHE

ll telefono cellulare deve possibilmente essere lasciato a casa, deve rimanere sempre spento e in cartella per l'intero tempo scuola. Nel caso in cui l'insegnante si accorga che il cellulare è acceso, è tenuto a ritirarlo e riporlo in una busta da far firmare all'alunno. La busta verrà poi consegnata in segreteria e potrà essere riconsegnata ai soli genitori.
In orario scolastico non si possono utilizzare dispositivi elettronici personali (I-pod, lettori MP3, etc.), salvo per fini didattici con l'autorizzazione dell'insegnante. Non è opportuno portare con sé oggetti di valore; la scuola non si assume alcuna responsabilità nel caso di eventuali smarrimenti e/o furti.
I docenti non devono lasciare incustoditi i PC, i Tablet e le LIM presenti nelle classi: devono inoltre utilizzarli seguendo le indicazioni previste (vd. Regole per l'utilizzo del pc e Circolare sull'uso dei Tablet).

Con questo atto s'intende attivare nella nostra scuola un regolamento in materia di "Tecnologie dell'Informazione e della Comunicazione" (TIC) da tutti accettata.

2. FORMAZIONE E CURRICOLO

La raccomandazione 2006/962/CE del Parlamento Europeo e del Consiglio dell'Unione Europea individua il quadro di riferimento europeo in materia di competenze chiave per l'apprendimento permanente. Tra queste è citata la competenza digitale, ovvero il "saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione per il lavoro, il tempo libero e la comunicazione". La competenza digitale è ritenuta quindi dall'Unione Europea competenza chiave, per la sua importanza e pervasività nel mondo d'oggi.

2.1. Curricolo sulle competenze digitali per gli studenti

"La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione 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" (Raccomandazione del Parlamento Europeo relativa alle competenze chiave per l'apprendimento permanente).

Dimensione tecnologica	Questo ambito fa riferimento a una serie di *skills* tecnologiche di base, come ad esempio la conoscenza di dispositivi e interfacce, ma comprende anche livelli più avanzati legati alla capacità di valutare le potenzialità dei contesti tecnologici in trasformazione, imparando a selezionare le soluzioni più opportune per affrontare ciascun compito;
Dimensione cognitiva	Comprende abilità legate al trattamento dell'informazione, dalla capacità di accedere, selezionare e interpretare dati a quella di valutarne criticamente la pertinenza e l'affidabilità, ma anche il saper trattare testi e dati per produrne sintesi, analisi e rappresentazioni con tabelle e grafici;
Dimensione etica	Questa dimensione riguarda il saper interagire con gli altri in modo corretto e responsabile, la circolazione del sapere online e il rispetto dei diritti di proprietà intellettuale, il tema dell'accessibilità e dell'inclusione.

In questa definizione emerge chiaramente come la competenza digitale (o *digital literacy)* non debba essere intesa in maniera riduttiva, solo come *expertise* tecnica, ma vada intesa come un costrutto complesso, in cui si intersecano dimensioni di natura diversa, che potremmo così schematizzare:

Dalla integrazione di queste tre principali dimensioni emerge un concetto di competenza digitale che fa riferimento alla capacità di comprendere e sfruttare l'effettivo potenziale delle TIC in un'ottica di costruzione di conoscenza e di promozione della partecipazione e dell'inclusione: il rapporto con le tecnologie digitali deve tendere ad un uso consapevole, critico e creativo.

Competenza digitale significa anche saper padroneggiare le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con "autonomia e responsabilità" nel rispetto degli altri e sapendone prevenire ed evitare i pericoli.

Intesa in questa accezione, la competenza digitale ed il suo curricolo sono necessariamente trasversali alle discipline previste dalle Indicazioni Nazionali, dal momento che tutte possono concorrere a costruirla ed in tutte si ritrovano abilità e competenze che fanno capo ad essa. Alla scuola spetta il compito di trovare raccordi efficaci tra la crescente dimestichezza degli alunni con le Tecnologie dell'Informazione e della Comunicazione e l'azione didattica quotidiana. Le TIC possono infatti offrire significative occasioni per sviluppare le competenze di comunicazione, collaborazione e *problem solving.*

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

1. conoscere e acquisire consapevolezza su natura, ruolo e opportunità delle TIC nella vita quotidiana e professionale;
2. distinguere il reale dal virtuale e riconoscere le correlazioni e le loro conseguenze;
3. sviluppare le abilità di base nelle TIC (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 TIC possono supportare 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 TIC (*netiquette, privacy*…).

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

Il comma 124 della Legge n. 107/2015 dispone: "Nell'ambito degli adempimenti connessi alla funzione docente, la formazione in servizio dei docenti di ruolo è obbligatoria, permanente e strutturale. Le attività di formazione sono definite dalle singole istituzioni scolastiche in coerenza con il piano triennale dell'offerta formativa e con i risultati emersi dai piani di miglioramento delle istituzioni scolastiche previsti dal regolamento di cui al decreto del Presidente della Repubblica 28 marzo 2013, n. 80, sulla base delle priorità nazionali indicate nel Piano nazionale di formazione, adottato ogni tre anni con decreto del Ministro dell'istruzione, dell'università e della ricerca, sentite le organizzazioni sindacali rappresentative di categoria." Il Piano di formazione del personale docente recepisce le criticità emerse dal RAV, le istanze provenienti dal PDM e le proposte di formazione di Enti ed Associazioni riconosciuti dal Miur.

Il corpo docente dell'IC IGEA ha partecipato, negli a.s. 2016/2017 e 2017/2018, a corsi di formazione nell'ambito di Piani Nazionali, oltre che ad iniziative organizzate dall'istituzione o dalle scuole associate in rete e possiede generalmente una buona base di competenze e nel caso delle figure di sistema, anche di carattere specialistico. E' inoltre disponibile ad aggiornarsi per mantenere al passo la propria formazione, in rapporto al rinnovo della dotazione multimediale. Il percorso complesso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica, non esauribile nell'arco di un anno

scolastico, può pertanto prevedere da un lato momenti di formazione interna (autoaggiornamento, momenti di formazione personale o collettiva anche all'interno dell'Istituto, con la condivisione delle conoscenze dei singoli e il supporto dell'Animatore digitale, la partecipazione alle iniziative promosse dall'Amministrazione centrale e dalle scuole polo), dall'altro formazione esterna, rispetto alla quale la scuola assicura tempestiva e capillare informazione su corsi, convegni e seminari che riguardino tali argomenti, cercando altresì di agevolare il personale che intenda parteciparvi.

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

Nell'Istituto i docenti hanno partecipato a diverse iniziative di formazione inerenti la *digital literacy*:

- corsi di formazione nell'ambito del Piano Nazionale Scuola Digitale, in particolare quelli relativi all'azione 14, 15 (Educazione ai media e ai social network, social media policy e uso professionale dei social media e Qualità, integrità e circolazione dell'informazione. Copyright e licenze aperte; ricerca, selezione e organizzazione di informazioni) 23, 24 (risorse educative aperte o OER);
- formazione relativa al progetto "*Hate speech e Media Education*": "BRICKS - Costruire il rispetto su internet combattendo l'*hate speech* "è un progetto europeo mirato a contrastare la diffusione *online* dei discorsi di istigazione all'odio nei confronti dei migranti, delle minoranze o altre categorie oggetto di discriminazione attraverso la *media education* e il coinvolgimento attivo dei fruitori e produttori di contenuti sul web".
- corsi del "Piano per la formazione dei docenti dell'ambito territoriale -21 Rimini" (Adottato dalla Conferenza di servizio di Ambito il 28.03.2017, in attuazione del Piano nazionale per la formazione dei docenti 2016/2019 e in risposta alle priorità formative indicate nei Rapporti di Autovalutazione (RAV) e Piani di Miglioramento (PdM} delle singole scuole.
- corsi sulla piattaforma docenti di Generazioni Connesse.

2.4. Sensibilizzazione delle famiglie

Il coinvolgimento dell'intera comunità scolastica è parte integrante del PTOF ed è una delle misure individuate nel piano d'azione presentato nell'ambito del progetto "Generazioni Connesse". L' Istituto attiverà iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. Saranno inoltre favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di *smartphone*, *chat line* e *social network* più diffusi, con particolare riferimento alla prevenzione del cyberbullismo. Allo scopo di mantenere viva l'attenzione delle famiglie sui tali temi, verranno inoltre valorizzate le opportunità di incontro e formazione per le famiglie sui temi oggetto della Policy, offerte dal territorio, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità ed avvalendosi anche della collaborazione della Polizia Postale e dell'ASL Romagna.

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

Le infrastrutture scolastiche non sono omogenee nei vari plessi dell'Istituto comprensivo per la distanza tra le varie strutture e per i supporti logistici che il comune di Bellaria Igea Marina fornisce alla scuola. Vi sono quindi situazioni differenti e regolamenti differenti adeguati alle situazioni.

La continua implementazione sia delle strumentazioni sia delle infrastrutture web rende necessario un continuo aggiornamento di questa sezione.

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

I PC fissi presenti nelle segreterie e nel laboratorio di informatica della scuola secondaria accedono alla rete internet tramite

connessione LAN (HDSL) utilizzando un'infrastruttura di proprietà del comune che la concede in comodato d'uso. A monte di questa struttura vi è un controllo a *white-list* con limitazioni che riguardano *social-network* e contenuti. E' presente sia sul server che su ogni singolo computer un antivirus aggiornato costantemente in remoto.
I PC fissi presenti nei laboratori di informatica del Plesso "A. Ferrarin" e "A. Manzi" sono collegati in rete tramite connessioni LAN; su ogni *router* che gestisce il traffico è attivo un *firewall* e su ogni singolo computer è installato un antivirus "Avast" versione free aggiornato ogni 6 mesi, un sistema anti-*malware* e anti-*spyware*, inoltre è attivo il web protector K9-Web protector.
I PC portatili si possono collegare via WI-FI tramite la rete "Linkem BIM-Scuola" a cui accedono solo i docenti con una password personale accreditata dall'ufficio tecnico del Comune di Bellaria Igea Marina detentore del contratto.
Su tutti i PC portatili della scuola è installato un antivirus "Avast" versione free aggiornato ogni 6 mesi, un sistema anti-*malware* e anti-*spyware*.

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

I PC portatili presenti nelle aule non richiedono una password di accesso per l'accensione. Ogni docente è quindi tenuto ad un controllo della strumentazione in aula, poiché l'uso del dispositivo è permesso agli alunni solo su autorizzazione dell'insegnante.
Ogni docente accede al registro elettronico attraverso una password personale che è a completa gestione dell'utente. L'accesso all'area riservata del sito web avviene tramite password personale per i docenti e gli assistenti amministrativi.
I PC della segreteria funzionano con una password generale a conoscenza solo dei servizi amministrativi, mentre il profilo amministratore è gestito dall'ufficio tecnico del Comune di Bellaria Igea Marina che ne detiene la password.
I PC del laboratorio di informatica della scuola secondaria hanno una password per utenti generici che i docenti comunicano agli studenti all'accesso, una password con privilegi da amministratore in possesso esclusivo dell'animatore digitale e una come amministratore dell'ufficio tecnico del Comune di Bellaria Igea Marina.
I PC della segreteria e i profili possiedono un backup remoto su un server fornito dal Comune di Bellaria Igea Marina presente nella loro sala CED.
I PC dei laboratori di informatica delle scuole primarie possiedono un profilo utente non protetto da password ed un profilo amministratore con password in possesso dell'animatore digitale e del professore referente dell'aula.
Come già detto, l'accesso alla rete wi-fi avviene tramite utenze personali per ogni docente pre-autorizzate dall'ufficio tecnico del Comune di Bellaria Igea Marina.

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 deve avvenire solo su autorizzazione del Dirigente scolastico e operativamente deve essere svolto dall'assistente amministrativo addetto. La posta elettronica è gestita tramite la piattaforma amministrativa Nuvola fornita dalla società Madisoft che applica sia filtri antivirus che antispam.

3.4. Blog e sito web della scuola

Il sito web della scuola è il mezzo prevalente per comunicare con le famiglie e condividere non solo le notizie, ma anche i progetti didattici svolti. I contenuti vengono gestiti da un gruppo di redattori che curano le diverse sezioni.
E' in corso l'implementazione dei documenti disponibili per i docenti nell'area riservata, alla quale accedono tramite

password personale.
La gestione tecnica è affidata all'animatore digitale in comunicazione con la ditta creatrice (Massimo Lenzi).

3.5. *Social Network*

Dall'anno 2017-18 l'istituto comprensivo, tramite delibera del Collegio Docenti, si è dotato di una pagina Facebook tramite la quale viene dato eco e risalto alle pubblicazioni del sito internet. Lo scopo che ha portato alla creazione della pagina è quello di raggiungere in maniera capillare e repentina le famiglie, soprattutto nel caso di comunicazioni urgenti sulla gestione della scuola e sulla tutela dei minori.
La gestione del profilo è compito della docente Paolucci che approva tutti i post prima della pubblicazione e controlla che vengano rispettate le linee guida interne che l'Istituto si è imposto sull'uso di immagini di minorenni all'interno della pagina Facebook.

3.6. Protezione dei dati personali

Il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Tutto il personale incaricato dal Dirigente Scolastico 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 (iscrizione a concorsi, partecipazione a laboratori, uscite e viaggi di istruzione).

4. STRUMENTAZIONE PERSONALE

L'uso di strumentazione personale all'interno dell'istituto comprensivo e comunque durante l'attività didattica mette in contrapposizione due aspetti molto importanti :la necessità di controllo, da parte del personale docente, delle informazioni (immagini, video, elaborati, ecc. …) che potrebbero violare il diritto di privacy e la possibilità di educare ad un utilizzo mirato e consapevole degli strumenti digitali.
E' necessario un regolamento che permetta la necessaria flessibilità tra una chiara regola di divieto che scoraggi l'abuso e la possibilità di utilizzo all'interno delle attività didattiche, tutelando i ragazzi e i docenti.

4.1. Per gli studenti: gestione degli strumenti personali - cellulari, *tablet* ecc..

L'utilizzo di strumentazione elettronica personale da parte degli studenti è definita all'interno del regolamento di istituto.
Non è consentito alcun uso di strumenti elettronici personali durante le attività didattiche, se non su precisa istruzione da parte del docente e comunque per uso didattico. Si può permettere l'utilizzo eccezionale del cellulare in caso di urgenza per comunicazioni tra gli alunni e le famiglie, sempre su autorizzazione e con controllo dell'identità dell'interlocutore da parte dell'insegnante.

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

Durante l'orario di lezione è consentito l'utilizzo di strumenti personali al solo scopo didattico-organizzativo (es. compilazione del registro elettronico), interfacciandoli anche con strumentazione presente nell'aula (LIM, proiettore, ecc.).
Non è consentito alcun uso di strumenti elettronici personali per scopi personali che distraggano dalla funzione docente e dalla vigilanza continua.

4.3. Per il personale della scuola: gestione degli strumenti personali - cellulari, *tablet* ecc..

Durante l'orario di servizio di tutto il personale ATA è consentito l'utilizzo del cellulare per comunicazioni di servizio e per comunicazioni personali urgenti.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

5.1. Prevenzione

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

Ciò fa sì che alcuni rischi che fanno parte del mondo digitale possano non essere percepiti come tali ed è dunque compito di adulti, famiglie ed insegnanti, affrontarli con l'obiettivo di prevenirli.

Tra i principali rischi, sia di carattere comportamentale che di ordine pratico, ricordiamo:

- ✓ 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).

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

5.2. Rilevazione

La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti.

Accorgersi tempestivamente di quanto accade e compiere azioni immediate di contrasto verso gli atti inopportuni –quando non illegali- diviene fondamentale per poter evitare conseguenze a lungo termine che possano pregiudicare il benessere e una crescita armonica dei soggetti coinvolti.

Laddove il docente colga possibili situazioni di disagio connesse ad uno o più di uno tra i rischi elencati nel paragrafo "Prevenzione", dovrà segnalare al Dirigente Scolastico il caso tramite la scheda di segnalazione appositamente predisposta e allegata al presente documento e potrà chiedere il supporto del Consiglio di Classe, degli operatori dello sportello d'ascolto, dei referenti del Cyberbullismo.

5.3. Gestione dei casi

A seguito della segnalazione, verrà avviato un colloquio tra le componenti scolastiche sopra elencate, finalizzato a valutare

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

RISCHI	AZIONI
Adescamento *online* (*grooming*)	Sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione. Qualora si venga a conoscenza di casi simili, occorre valutarne la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.
Cyberbullismo	Campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni. I casi possono essere molto variegati, variando dal semplice scherzo di cattivo gusto via sms/Whatsapp a vere e proprie minacce verbali e fisiche, che costituiscono reato. Occorre confrontarsi con il Dirigente Scolastico sulle azioni da intraprendere.
Dipendenza da Internet, videogiochi, shopping o *gambling online*	Informazioni sul fatto che ciò può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito a insaputa di altri) rappresenta un vero e proprio illecito.
Esposizione a contenuti pornografici, violenti, razzisti	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione e sensibilizzazione sulla necessità di monitorare l'esperienza online dei propri figli. Verso gli alunni: inserimento nel curricolo di temi legati alla affidabilità delle fonti online, all'interculturalità e al rispetto delle diversità. Qualora si venga a conoscenza di casi simili, occorre convocare i genitori per richiamarli a un maggiore controllo sulla fruizione di Internet da parte dei propri figli e/o sulla necessità di non usufruirne in presenza degli stessi.
Sexting e pedopornografia	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione. Verso gli alunni: inserimento nel curricolo di temi legati all'affettività, alla sessualità e alle differenze di genere. In casi simili, se l'entità è lieve occorre in primo luogo parlarne con alunne e alunni e rispettivi genitori, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale

	configura il reato di distribuzione di materiale pedopornografico. Chi è immerso dalla nascita nelle nuove tecnologie spesso non è consapevole che una foto o un video diffusi in rete potrebbero non essere tolti mai più né è consapevole di scambiare o diffondere materiale pedopornografico. In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico per gli adempimenti del caso.
Violazione della *privacy*	Informazione sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farle rispettare. Se il comportamento rilevato viola solo le norme di buona convivenza civile e di opportunità, occorre convocare i soggetti interessati per informarli e discutere dell'accaduto e concordare forme costruttive ed educative di riparazione. Qualora il comportamento rappresenti un vero e proprio illecito, il Dirigente Scolastico deve esserne informato in quanto a seconda dell'illecito sono previste sanzioni amministrative o penali.

Annessi

1. Modulo di rilevazione casi.
2. Schema riepilogativo delle situazioni gestite legate a rischi online.
3. Mappa operativa delle azioni da intraprendere in caso di *cyberbullismo*.
4. Questionario d'Istituto di indagine su bullismo/*cyberbullismo*.

FIRMA REFERENTI

Prof.ssa Sara COTTI

Annamaria AUTIERO

COMPRENSIVO STATALE IGEA ISTITUTO SCOLASTICO - SCUOLA DELL'INFANZIA - SCUOLA PRIMARIA - SCUOLA SEC. DI I° GRADO - IGEA MARINA (RN) BELLARIA

IL DIRIGENTE SCOLASTICO

Dott.ssa Myriam TOCCAFONDO

Classe _____	Istituto (se plesso) _____		
Data _____	*Ora* _____	*Luogo* _____	*riferito da?* _____
Cosa è successo?			
Responsabile/i		Vittima/e	
			Firma _____
Aggiornamento 1			
Aggiornamento 2			
Aggiornamento 3			

Co-financed by the European Union
Connecting Europe Facility

Generazioni Connesse

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?		

Cosa fare in caso di... cyberbullismo?

CASO A (SOSPETTO) - Il docente sospetta che stia accadendo qualcosa tra gli alunni/e della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

ATTORI ADULTI DA COINVOLGERE

1. Condividi con il referente per il cyberbullismo (e/o il referente indicato nell'e-policy): valuta con lui/loro le possibili strategie di intervento. - proposta di commissione con referente per plesso
2. Valuta se è il caso di avvisare il consiglio di classe.
3. Valuta se è il caso di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.
4. Sonda il clima di classe, ascoltando i ragazzi e monitorando ciò che accade (ma senza fare indagini o interrogatori)
5. Cerca di capire il livello di diffusione dell'episodio a livello di Istituto.
   - chiedere in classe, sondando tra gli studenti

CLASSE/I DA COINVOLGERE

1. **Dialoga** (con la classe - 1): Parla del cyberbullismo e delle sue conseguenze (non nominare gli alunni che sospetti coinvolti). Suggerisci di **chiedere aiuto** per situazioni di questo tipo. Prevedi un momento laboratoriale (suggerimenti utili qui: link al lesson plan sulla piattaforma generazioni connesse)

Se ancora non ci sono evidenze, previeni:

1. **lavora con la classe sul clima** (con la classe - 3): Proponi attività in classe sull'empatia e sul riconoscimento delle emozioni (proprie e altrui)
2. Informa gli alunni su ciò che dice la **legge italiana** sul cyberbullismo - nel caso chiedi aiuto al referente CB (predisporre delle slide)
3. **Continua a monitorare la situazione**

Se hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla **helpline** del progetto Generazioni Connesse, al numero gratuito **1.96.96.**

anche se non riscontri nulla, promuovi per l'intera comunità scolastica percorsi di prevenzione dei comportamenti a rischio online

se riscontri situazioni di bullismo o cyberbullismo passa al CASO B

CASO B (EVIDENZA) - Il docente ha evidenza che stia accadendo qualcosa tra gli alunni/e della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Se hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in ogni momento Una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 - Operativo h 24

ATTORI ADULTI DA COINVOLGERE

1. Condividi con il referente per il cyberbullismo (e/o il referente indicato nell'e-policy): valuta con lui/loro le possibili strategie di intervento.
2. Avvisa il Dirigente Scolastico che convoca il CDC.
3. Se non c'è fattispecie di reato
   - Richiedi la consulenza dello psicologo/a scolastico a supporto della gestione della situazione, in base alla gravità
   - Informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto), se possibile con la presenza dello psicologo/a, su quanto accade e condividete informazioni e strategie.
   - Informa i genitori di ragazzi/e infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy)
   - Attiva il consiglio di classe.
   - **Valuta come coinvolgere** gli operatori scolastici su quanto sta accadendo.

A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnala alla **Polizia Postale:** a) contenuto ; b) modalità di diffusione

Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).

Promuovi per l'intera comunità scolastica percorsi di prevenzione dei comportamenti a rischio online

CLASSE/I DA COINVOLGERE

1. Capire il livello di diffusione dell'episodio a livello di Istituto e parla della necessità di **non diffondere** ulteriormente online i materiali.
2. **Dialoga** (con la classe - 1): Parla del cyberbullismo e delle sue conseguenze (non nominare gli alunni coinvolti). Suggerisci di **chiedere aiuto** per situazioni di questo tipo. Prevedi un momento laboratoriale in modo da facilitare l'elaborazione della situazione.
3. **Dialoga** (con la classe - 2): a seconda della situazione trova il modo di supportare la vittima e di responsabilizzare i compagni, rispetto al loro ruolo, anche di spettatori, nella situazione. A seconda del livello di diffusione anche nelle altre classi

Tieni traccia di quanto successo e delle azioni intraprese: **compila il diario di bordo**

SONDAGGIO ANONIMO SULLE PREPOTENZE A SCUOLA

1. Hai subito delle prepotenze da ragazzi/ragazze a scuola, in questi ultimi tre mesi?

☐ mai successo in questo periodo
☐ una o due volte
☐ poche volte
☐ diverse volte
☐ spesso

2. Se sì, che cosa è successo? (anche più di una risposta)

☐ mi hanno dato pugni, calci o spinte in modo continuativo
☐ mi hanno minacciato di farmi qualcosa di spiacevole
☐ hanno rovinato apposta delle mie cose personali (abbigliamento, zaino, quaderno, libro,…)
☐ mi hanno obbligato a dare loro dei soldi
☐ mi hanno derubato
☐ mi hanno offeso pesantemente con parolacce o prese in giro umilianti
☐ hanno messo in giro storie false e bugie su di me
☐ mi hanno escluso dal gruppo solo per ferirmi
☐ mi hanno obbligato a fare qualcosa di umiliante
☐ ho subito altri tipi di prepotenze *(specifica quali nelle righe sotto)*

_____

_____

3. Coloro che hanno agito queste prepotenze:

☐ sono della mia classe ☐ sono di altre classi ☐ sia della mia classe che di altre

4. Ti sei mai reso responsabile di prepotenze verso qualcuno?

☐ mai ☐ qualche volta ☐ spesso ☐ mai, però ho assistito a prepotenze verso altri

5. Negli ultimi tre mesi, hai subito offese, molestie o minacce da parte di qualcuno attraverso internet, cellulare o altro mezzo digitale? *(fuori dalla scuola)*

☐ non è mai successo in questo periodo
☐ è successo una o due volte
☐ è successo poche volte
☐ è successo diverse volte
☐ è successo spesso

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

☐ mi hanno inviato dei messaggi volgari, offensivi o minacciosi
☐ hanno pubblicato on-line dei segreti che avevo confidato, per danneggiare i miei rapporti di amicizia o la mia reputazione
☐ hanno scritto di me cose non vere, falsità, inventate apposta 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
☐ ho subito altri tipi di prepotenze… *(specifica quali nella riga sotto)*

_____

7. Hai fatto prepotenze on-line (come quelle scritte sopra) verso qualcuno?

☐ mai ☐ qualche volta ☐ spesso ☐ mai, però ho assistito a prepotenze verso altri

8. Sempre in questi ultimi mesi, sai se è accaduto qualcosa attraverso internet, chat o social, che ha fatto star male qualcuno che conosci? Scrivi che cosa è accaduto:

_____

_____