



ISTITUTO COMPRENSIVO - "MASSARI - GALILEI"-BARI
Prot. 0002897 del 18/05/2018
(Uscita)

Policy di E-Safety

a.s. 2018/2019



INDICE

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 i regolamenti esistenti

2. FORMAZIONE DEL 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 TIC 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 la componente studentesca: gestione degli strumenti personali (cellulari, tablet, ecc.)
- 4.2 Per il personale docente/ATA: gestione degli strumenti personali (cellulari, tablet ecc.)
- 4.3 Utilizzo del laboratorio di informatica e delle postazioni di lavoro

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

1. INTRODUZIONE

1.1. Scopo della policy

L'Istituto Comprensivo "Massari Galilei" ha aderito al progetto "Generazioni Connesse", promosso dal MIUR per offrire alle Istituzioni Scolastiche interessate un supporto effettivo nella definizione di misure di prevenzione, rilevazione e gestione delle problematiche derivanti da un uso non consapevole delle tecnologie digitali tra gli studenti, anche attraverso la formazione degli insegnanti e la sensibilizzazione dei genitori.

La scuola accoglie minori "nativi digitali" che hanno un'innata predisposizione all'uso delle tecnologie, tuttavia, assai frequentemente a questa abilità non corrisponde una adeguata e corretta capacità interpretativa della mole di informazioni alla quale essi sono di continuo sottoposti, pertanto sono spesso esposti a rischi di cui sono inconsapevoli.

Il presente documento nasce dunque dall'esigenza di promuovere un uso sicuro e consapevole delle TIC, in ambiente scolastico e nella didattica, e dalla necessità di prevenire e gestire situazioni problematiche connesse all'uso delle tecnologie digitali.

Il documento potrà, se necessario, essere modificato e aggiornato annualmente in funzione di eventuali nuove esigenze e, conseguentemente, di nuove azioni da porre in essere anche nell'ottica di una sua piena integrazione con obiettivi e contenuti degli altri documenti di Istituto, principalmente il PTOF e il Regolamento di Istituto.

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

Dirigente Scolastico

È responsabile della presentazione di questo documento all'attenzione del Consiglio di Istituto e al Collegio dei Docenti entro la fine dell'a.s. 2017/18. Deve valutare l'efficacia della policy e monitorarne/indirizzarne l'attuazione, anche in collaborazione con il personale scolastico, gli enti locali e gli stakeholder territoriali. A tale scopo necessita di ricevere tempestive informazioni sulle violazioni al presente regolamento o eventuali problemi attualmente non noti dal corpo docente o dal personale ATA che ne vengano a conoscenza.

Nella promozione dell'uso consapevole della rete, il Dirigente Scolastico deve:

- garantire la corretta formazione del personale scolastico sulle tematiche relative all'uso sicuro e consapevole di internet e della rete;
- garantire una formazione adeguata del personale docente relativo all'uso delle TIC nella didattica;

- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line.

Animatore digitale

L'Animatore digitale, supportato dal Team dell'innovazione, deve:

- stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on line e alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione);
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti alla "scuola digitale".

Personale docente

È compito dei docenti:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantire che gli alunni comprendano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;
- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;

- controllare 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, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo all'Animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- segnalare al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.

Personale A.T.A.

È compito del personale A.T.A.:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica, la policy dell'Istituto e le relative buone pratiche;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico e/o all'animatore digitale per i provvedimenti di competenza.

Componente studentesca

Gli alunni sono responsabili del corretto utilizzo dei sistemi informatici e della tecnologia digitale, in accordo con i termini previsti da questa policy. In particolare, sono tenuti a:

- utilizzare in modo responsabile, in relazione al proprio grado di maturità e di apprendimento, le tecnologie digitali in conformità con quanto richiesto dai docenti;
- avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;
- comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori;

- non utilizzare dispositivi personali durante le attività didattiche se non espressamente consentito dal personale docente;
- comprendere l'importanza della segnalazione di ogni abuso, uso improprio o accesso a materiali inappropriati ed essere consapevoli del significato e della gravità del cyber-bullismo.

Genitori

È fondamentale che i genitori/tutori/affidatari sostengano la linea di condotta adottata dalla scuola nei confronti dell'utilizzo delle TIC nella didattica e che concordino 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.

La scuola coglierà ogni occasione per sensibilizzare i genitori sull'uso corretto del web attraverso incontri con la Polizia Postale ed altri esperti o educatori, circolari, sito istituzionale e altre comunicazioni telematiche, informazioni su campagne di sicurezza promosse da altre istituzioni o su convegni dedicati a questo tema. I genitori saranno incoraggiati a sostenere la scuola nel promuovere le buone pratiche di e-safety e a seguire le linee guida sull'uso appropriato di:

- immagini digitali e video registrati in occasione di eventi scolastici, anche al di fuori dei locali scolastici;
- accesso alle sezioni del sito dedicate ai genitori, con particolare riguardo al registro elettronico;
- uso dispositivi personali dei loro figli nella scuola (quando è consentito).

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

Per evitare che l'adozione di questa policy rappresenti un mero atto formale, l'Istituto si impegna a prendere spunto da essa come base di partenza per una serie di azioni e iniziative. A partire dalla pubblicazione sul sito della scuola, si possono ipotizzare per esempio:

Per il corpo docente

- discussione collegiale sui contenuti, sulle pratiche indicate e su come inserire nel curriculum le tematiche di interesse della policy;
- un confronto collegiale, su base annuale, circa la necessità di apportare modifiche e miglioramenti alla policy vigente;
- elaborazione di protocolli condivisi di intervento.

Per la componente studentesca

- la discussione in classe della policy nei primi giorni di scuola, con particolare riguardo al protocollo di accoglienza per le nuove classi prime;

- l'affissione di un estratto di questo documento in ogni classe, in particolare dei comportamenti da attuare in caso di bisogno.

Per i genitori

- l'organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare, da adottare e da evitare.

1.4 Gestione delle infrazioni alla policy

Disciplina degli alunni.

Art. 35 del Regolamento d'Istituto: "Divieto di uso del telefono cellulare e connessione a siti web non autorizzati".

All'interno dell'edificio scolastico e durante lo svolgimento delle lezioni è assolutamente vietato usare telefoni cellulari e altri dispositivi elettronici non autorizzati. Inoltre, è assolutamente vietato, con computer della scuola o personali, la connessione a siti web non autorizzati dal docente, in particolare è severamente vietato connettersi a siti di contenuto immorale.

Le potenziali infrazioni a carico degli alunni sono identificabili in:

- Uso del telefono cellulare o altri dispositivi elettronici all'interno dell'edificio scolastico senza autorizzazione.
- Diffusione non autorizzata di foto e filmati che violino la privacy o siano offensivi e non rispettosi della dignità della persona.
- Connessioni a siti proibiti o comunque non autorizzati.

Art. 36 del Regolamento d'Istituto: "Le sanzioni".

Le sanzioni disciplinari hanno esclusivamente finalità educative e tendono al rafforzamento del senso di responsabilità, al ripristino di rapporti corretti all'interno della comunità scolastica. Le sanzioni sono sempre temporanee e proporzionate all'infrazione, tengono sempre conto della situazione dell'alunno e gli garantiscono il diritto di difesa prima dell'applicazione della sanzione.

Riguardo il procedimento sanzionatorio si fa riferimento all'art. 1 del D.P.R. 21 novembre 2007, n. 235 - Regolamento recante modifiche ed integrazioni al decreto del Presidente della Repubblica 24 giugno 1998, n. 249, concernente lo statuto delle studentesse e degli studenti della scuola secondaria.

Disciplina del personale scolastico

Il personale scolastico, in particolare i docenti, dovranno favorire un utilizzo corretto e responsabile delle TIC da parte degli alunni, evitando di incorrere loro stessi in potenziali infrazioni quali:

- utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività d'insegnamento, anche tramite installazione di software o il salvataggio di materiali non idonei;
- trattamento dei dati personali sensibili degli alunni non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC.

Il D.S. ha la facoltà di revocare l'accessibilità temporanea o permanente ai laboratori informatici e/o all'utilizzo di strumenti tecnologici, nel caso in cui non ci si attenga alle regole stabilite.

Il D.S. può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso ad internet, ma non alla posta elettronica personale, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone una copia per eventuali successive investigazioni. Tutto il personale è tenuto a collaborare con il D. S. 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 rilevate. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

Disciplina dei genitori

I genitori dovranno favorire un utilizzo corretto e responsabile delle TIC da parte dei propri figli sia a casa sia a scuola, collaborando e sostenendo l'istituzione scolastica nel rispetto e nella condivisione delle scelte educative.

Dovranno, inoltre, prendere visione del presente documento (Policy E-Safety), in particolar modo della sezione riguardante la *disciplina degli alunni* al punto 1.4 "Gestione delle infrazioni alla policy", consultandolo sul sito web della scuola.

1.5 Monitoraggio dell'implementazione della policy e suo aggiornamento

Il monitoraggio dell'implementazione della Policy sarà curato dal Dirigente scolastico, dai Responsabili delle azioni di contrasto al cyberbullismo, dall'Animatore Digitale e dai Collaboratori del Dirigente, al termine dell'anno scolastico, contestualmente al Rapporto di Autovalutazione e sulla base dei casi problematici riscontrati e della loro gestione.

1.6 Integrazione della policy con i regolamenti esistenti

Il presente documento verrà allegato al Regolamento d'Istituto e pubblicato sul sito web della scuola.

2. FORMAZIONE E CURRICOLO

2.1 Curricolo sulle competenze digitali per gli studenti

Secondo le *Indicazioni Nazionali*, in raccordo con il *Programma Europeo per le Competenze chiave in un mondo in trasformazione*, al termine del primo ciclo di istruzione, lo studente deve possedere buone competenze digitali e saper usare consapevolmente le tecnologie della comunicazione.

Le Tecnologie dell'Informazione e della Comunicazione preparano gli studenti ad un'attiva e consapevole partecipazione ad un mondo in rapida evoluzione e nel quale è necessario acquisire abilità e competenze in grado di facilitare l'adattamento dell'individuo ai continui cambiamenti.

Alla Scuola spetta il compito di trovare raccordi efficaci tra la crescente dimestichezza degli alunni con le TIC e l'azione didattica quotidiana. Pertanto l'uso delle TIC dovrà essere inserito nel curricolo sia a livello disciplinare sia a livello interdisciplinare, strutturandolo in modo da rendere gli alunni in grado di:

- cercare, esplorare, scambiare e presentare informazioni in modo responsabile, creativo e con senso critico;
- avere un rapido accesso a idee ed esperienze provenienti da persone, comunità e culture diverse;
- essere criticamente consapevoli dei materiali che si leggono sul web, attraverso la ricerca e l'analisi di informazioni e dati che possano aiutarlo a distinguere quelli attendibili da quelli che necessitano di approfondimento, di controllo e di verifica;
- impiegare materiali prelevati da internet a scopi didattici conformemente al diritto d'autore;
- segnalare contenuti sgradevoli o illegali.

Nel corso dell'anno sono state realizzate le seguenti attività in relazione ai sopraddetti obiettivi:

- partecipazione alla 5° Campagna itinerante "Una Vita da Social", organizzata dal Ministero dell'Interno – Dipartimento della Pubblica sicurezza; gli operatori della Polizia Postale hanno incontrato gli alunni delle classi prime di scuola secondaria di I grado e illustrato loro le più frequenti insidie del web (cyberbullismo, sexting, adescamenti on line);
- partecipazione al progetto "Radio Kreattiva", proposto dall'associazione Kreattiva per sensibilizzare gli studenti sui temi della legalità, diffondere la pratica di cittadinanza attiva e stimolare il protagonismo sociale nelle scuole; gli alunni della classe 1^H hanno incontrato diversi "testimoni della legalità" e affrontato temi quali l'importanza di un uso positivo della Rete Internet e dei *social*;
- attività di *Coding* in alcune classi della scuola primaria e secondaria relativamente allo sviluppo del pensiero computazionale.

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

Nell'ottica degli obiettivi strategici individuati dalla Comunità Europea, legati al ruolo delle tecnologie dell'informazione e della comunicazione nell'esperienza quotidiana delle nuove generazioni, molto docenti del nostro Istituto hanno aderito ad iniziative atte a raggiungere un buon livello di formazione in merito all'utilizzo e all'integrazione delle TIC nella didattica. Inoltre, il nostro Istituto ha aderito ad un'iniziativa del Municipio II di Bari volta alla sensibilizzazione, formazione e informazione di alunni, docenti e genitori riguardo l'uso consapevole di internet e alle problematiche legate al fenomeno del cyber bullismo. Il prodotto finale di questo percorso, un video realizzato dagli alunni, è stato pubblicato sulla piattaforma di Generazioni Connesse.

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

Il percorso della formazione specifica dei docenti sull'utilizzo consapevole di internet prevede momenti di auto aggiornamento, di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione cui accedono sempre più ed autonomamente anche i ragazzi.

Nell'a.s. 2018/19 verranno attivate due classi prime digitali di scuola secondaria di I grado, una nel plesso Massari e una nel plesso Galilei, con uso di iPad personali a scuola secondo il metodo del BYOD (Bring your own device). I docenti stanno seguendo una specifica formazione su "Ambienti digitali e BYOD" tenuti da personale qualificato esterno alla scuola, che consentirà loro di innovare la didattica con l'uso delle tecnologie digitali.

Viene favorita anche la partecipazione ad iniziative al di fuori della pianificazione d'Istituto, in coerenza con le finalità e gli obiettivi del Piano di Formazione.

La scuola ha inoltre organizzato, come capofila, un protocollo di intesa tra una rete di 30 scuole e le Associazioni Penelope Onlus e Gens Nova Onlus, che da anni svolgono attività di prevenzione ed informazione all'interno dei vari Istituti scolastici della Regione Puglia, in tema di contrasto al bullismo, cyberbullismo ed altre forme di violenza. In quest'anno scolastico verrà presentato il progetto di formazione "Bullismo e cyberbullismo alla luce della recente normativa: proposte e suggerimenti operativi", rivolto a dirigenti scolastici, docenti referenti per il cyberbullismo, collaboratori del DS e referenti di sede delle 30 scuole in rete, che poi verrà realizzato nei mesi di settembre e ottobre.

Sulla homepage del sito scolastico www.smsmassarigalileibari.gov.it è possibile trovare materiali informativi, progetti ed iniziative intraprese dalla scuola riguardanti la tematica in oggetto. Nel sito è presente la sezione "Newsletter Spazio Genitori" nella quale vengono pubblicati contributi da parte di *genitori esperti* (psicoterapeuti - professionisti della comunicazione - ecc.) anche sul tema della sicurezza on-line.

2.4 Sensibilizzazione delle famiglie

In quest'ottica di comunità di apprendimento il comitato della "Newsletter Spazio Genitori" ha già organizzato numerosi incontri sul tema, che continueranno in futuro con ulteriori approfondimenti.

In questo anno scolastico è stato istituito il "Comitato Genitori Massari-Galilei", costituito dai rappresentanti dei genitori in Consiglio di Istituto e nei Consigli di classe, che ha in calendario, tra l'altro, numerosi interventi finalizzati al confronto e alla discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo.

La scuola, attraverso documentazione informativa e organizzazione di incontri, coinvolge le famiglie per sensibilizzarle ad un corretto uso delle nuove tecnologie da parte dei ragazzi a casa e a scuola. Nel mese di dicembre la scuola ha organizzato il convegno "L'abuso sui minori nell'era della webcrazia", rivolto a docenti e famiglie e aperto al territorio, durante il quale relatori autorevoli hanno parlato delle insidie della rete.

3 GESTIONE DELL' INFRASTRUTTURA E DELLA STRUMENTAZIONE TIC DELLA SCUOLA

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

L'accesso a internet è possibile e consentito per la didattica nelle classi dotate di LIM e PC portatili e nei laboratori multimediali. Il docente dalla propria postazione, tramite apposito software, può controllare l'operato di ciascun utente. Le postazioni non sono dotate di webcam. Agli alunni non è consentito accedere alla rete internet della scuola con i propri dispositivi personali. Solo gli iPad degli alunni delle classi prime digitali a.s. 2018/19 verranno connessi alle rete WiFi scolastica.

È prevista l'installazione di filtri per impedire collegamenti a siti non idonei alla didattica.

L'aggiornamento del sistema informatico dei laboratori e la manutenzione della strumentazione TIC della scuola, ove necessario, sono affidati a tecnici esterni.

3.2 Gestione accessi (password, backup, ecc.)

Le reti WiFi della scuola necessitano di password per l'accesso, che è stata comunicata a docenti e personale A.T.A. ma che non può essere comunicata ad alunni o a terzi.

Gli ambienti di segreteria e la presidenza utilizzano una rete internet differente rispetto a quella utilizzata per la didattica.

I computer portatili presenti nelle aule della scuola secondaria non richiedono la password di accesso per l'accensione, a differenza di quelli nella primaria. Ogni docente è

tenuto al controllo della strumentazione in aula e l'uso del dispositivo è permesso agli alunni solo su autorizzazione.

I docenti accedono al registro elettronico e al sito web istituzionale attraverso password personali che non possono essere comunicate a terzi.

3.3 E-mail

L'accesso alla posta elettronica istituzionale MIUR può essere effettuato solo dal personale di segreteria e dalla presidenza utilizzando credenziali uniche.

L'uso di e-mail personali viene favorito come mezzo di diffusione di comunicati e notifiche di circolari d'Istituto pubblicate sul sito istituzionale.

3.4 Blog e sito web della scuola

Il sito web dell'Istituto è gestito dal Dirigente Scolastico e dall'Animatore Digitale, non è invece attivo alcun blog. Il sito istituzionale con estensione "gov.it" ha diversi siti tematici che rimandano al contenuto di interesse (Pubblicità legale, Comunicazioni, bacheca Sindacale ecc.). Sul sito è possibile trovare Regolamenti, materiali didattici, pubblicizzazione di eventi, documentazione di attività curricolari ed extracurricolari svolte. Pulsanti attivi permettono l'accesso a link di interesse tra cui il Registro Elettronico.

È possibile accedere all'area riservata del sito dove sono caricate le comunicazioni interne e la documentazione didattica, che vengono inviate anche attraverso l'account istituzionale Google Apps ad ogni docente. L'accesso a tale area è nominativo.

3.5 Social Network

Attualmente è in uso una pagina Facebook gestita dal Dirigente Scolastico che in tempo reale provvede a postare circolari e comunicazioni di interesse delle famiglie e degli alunni, nonché a rispondere a domande poste in modalità privata.

Sul social vengono pubblicizzate anche le attività e gli eventi occorsi.

3.6 Protezione dei dati personali

L'Istituto Comprensivo "Massari-Galilei" rispetta la privacy dei propri utenti e si impegna a proteggere i dati personali forniti dagli stessi. La raccolta e il trattamento dei dati personali avvengono in seguito alla richiesta di servizi da parte dell'utente e sono trattati in conformità alla normativa vigente. La comunicazione di tali dati a terzi avverrà solo a seguito di consenso dell'utente.

4. STRUMENTAZIONE PERSONALE

4.1 Per la componente studentesca: gestione degli strumenti personali (cellulari, tablet ecc.)

- Agli alunni della scuola secondaria di I grado è consentito di portare il telefono cellulare a scuola solo per motivi familiari e organizzativi. Coerentemente con quanto indicato dalla Direttiva Ministeriale n. 30 del 15 marzo 2007, gli studenti sono però tenuti a tenere il cellulare spento durante tutto il periodo di permanenza a scuola e in ogni ambiente. I cellulari, i tablet e le relative fotocamere e registratori vocali non verranno utilizzati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate dal corpo docente.
- Nel caso in cui gli alunni debbano comunicare con la famiglia durante l'orario scolastico, la scuola dà loro la possibilità di usare gratuitamente la linea fissa rivolgendosi a un collaboratore; allo stesso modo le famiglie devono chiamare il centralino della scuola se hanno assoluta necessità di parlare con i propri figli. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.
- Gli studenti delle classi digitali sono autorizzati ad utilizzare il tablet in classe esclusivamente per uso didattico, secondo le indicazioni dei docenti, i quali provvederanno a monitorare e controllare l'utilizzo del dispositivo.
- In ogni classe, le famiglie degli alunni con disturbi specifici di apprendimento concorderanno con il Consiglio di Classe le modalità di impiego di strumenti compensativi quali tablet e computer portatili e le modalità di controllo e custodia degli stessi.
- L'invio di materiali abusivi, offensivi o inappropriati è vietato, anche se avviene all'interno di cerchie o gruppi di discussione privati.

4.2 Per il personale docente/A.T.A.: gestione degli strumenti personali (cellulari, tablet ecc.)

Per i docenti:

- Durante le ore di lezione non è consentito l'utilizzo del telefono cellulare, mentre è consentito l'uso di altri dispositivi elettronici personali a scopo didattico ed integrativo di quelli scolastici disponibili. Durante il restante orario di servizio è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente mentre è permesso l'uso di altri dispositivi elettronici personali per attività funzionali all'insegnamento, ad integrazione di quelli scolastici disponibili.
- Le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali.
- La password di accesso alla rete wireless va custodita con cura e per nessuna ragione deve essere divulgata a chi non ha titolo per utilizzarla (studenti, genitori, operatori esterni).
- Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (pendrive, hard disk esterni) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.

Per il personale A.T.A.:

- Durante l'orario di servizio è consentito l'utilizzo del telefono cellulare solo per comunicazioni personali di carattere urgente.

- Le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali.
- La password di accesso alla rete wireless va custodita con cura e per nessuna ragione deve essere divulgata a chi non ha titolo per utilizzarla (studenti, genitori, operatori esterni).

4.3 Utilizzo del laboratorio di informatica e delle postazioni di lavoro

La scuola dispone di 3 laboratori di informatica (uno per ogni plesso) e di una postazione computer in ogni sala docenti, oltre che di PC laptop per ogni aula provvista di LIM. Le apparecchiature presenti nella scuola sono patrimonio comune e vanno utilizzate con il massimo rispetto. Pertanto, per il loro utilizzo, è necessario attenersi alle seguenti disposizioni:

- I laboratori informatici e le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.
- Quando un docente, da solo o con la classe, usufruisce del laboratorio di informatica, deve obbligatoriamente registrare il proprio nome e l'eventuale classe nell'apposito registro delle presenze di laboratorio, indicando l'orario di ingresso, quello di uscita e 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.
- L'ingresso degli allievi nei laboratori è consentito solo in presenza di un docente.
- Il docente accompagnatore è responsabile del corretto utilizzo di hardware e software.
- Docenti e alunni non sono autorizzati ad installare software o applicazioni sui PC della scuola. Questa attività può essere svolta esclusivamente dall'animatore digitale o dai responsabili dei laboratori di informatica. I docenti pertanto dovranno rivolgersi all'animatore digitale o al responsabile del laboratorio per l'installazione di software o applicazioni per uso didattico.
- Durante l'attività didattica è opportuno che ogni insegnante dia chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforma studenti ecc.), condividendo con gli studenti la netiquette e indicandone le regole;
- Nei laboratori è vietato utilizzare CD personali, pendrive o altri dispositivi se non dopo opportuno controllo con sistema di antivirus aggiornato.
- All'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il locale in ordine e le macchine spente correttamente.
- In caso di malfunzionamento o guasto dei PC bisogna darne tempestiva segnalazione al responsabile del laboratorio.
- Agli studenti non è consentito conoscere la password di accesso alla rete internet della scuola.
- Il Responsabile di laboratorio che verifichi un uso improprio del laboratorio è tenuto a darne tempestiva comunicazione per iscritto al Dirigente Scolastico.
- Agli alunni è severamente vietato l'utilizzo delle postazioni presenti in sala docenti.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

Il primo passo che la nostra scuola intraprenderà sarà quello del coinvolgimento della comunità scolastica in percorsi di prevenzione dei comportamenti online a rischio.

La scuola si avvale della collaborazione di enti, associazioni, forze dell'ordine, per realizzare incontri rivolti alla componente studentesca e alle famiglie con l'intento di fornire ogni elemento utile alla prevenzione e alla gestione dei problemi relativi alla sicurezza informatica; le famiglie sono invitate a proporre tematiche di particolare interesse su cui la scuola focalizzerà il proprio intervento.

La scuola attiva inoltre uno sportello di ascolto al quale la componente studentesca, le famiglie, il personale scolastico possono rivolgersi per avere consigli e sostegno psicologico, anche relativamente alle tematiche del cyberbullismo.

Le misure di prevenzione comprendono, oltre alla formazione, l'integrazione nel curriculum dei temi legati al corretto utilizzo delle TIC e di Internet. La progettazione di unità didattiche specifiche deve essere pianificata a livello di dipartimenti disciplinari, garantendo un intervento su ogni classe, anche con docenti non titolari della classe. Si demanda ai dipartimenti disciplinari la scelta dei settori su cui focalizzare la formazione: a titolo di esempio il dipartimento letterario si può soffermare in particolare sugli aspetti legati all'affettività, alla socializzazione e alla cittadinanza, quello tecnologico-scientifico-matematico sulle questioni tecniche relative al legame causale tra salute ed uso delle tecnologie, quello di arte/musica sulla tutela del diritto d'autore, il docente di tecnologia sugli aspetti tecnici legati all'uso delle TIC, ecc.

A partire dalla corretta formazione e sensibilizzazione, è compito di tutti gli adulti coinvolti (docenti e personale A.T.A.), secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti, essere confidenti e custodi, diretti o indiretti, di ciò che i ragazzi vivono, evitando con cura ogni atteggiamento accusatorio o intimidatorio per riuscire a ricevere dai minori più fragili segnalazioni e confidenze circa situazioni problematiche vissute. La rilevazione dei casi è compito dell'intera comunità educante.

I docenti in particolare sono chiamati a essere particolarmente attenti nell'osservazione delle dinamiche di classe, primi moderatori delle problematiche, dei rischi, dei pericoli che i bambini e gli adolescenti possono vivere e affrontare ogni giorno. Accorgersi tempestivamente di quanto accade e compiere azioni immediate di contrasto verso gli atti inopportuni - quando non illegali - diviene fondamentale per poter evitare conseguenze a lungo termine che possano pregiudicare il benessere e una crescita armonica dei soggetti coinvolti.

La gestione dei casi rilevati va differenziata a seconda della loro gravità; fermo restando che è opportuna la condivisione a livello di Consiglio di Classe di ogni episodio rilevato, anche minimo. Alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe. Altri casi ancora possono essere affrontati convocando genitori e alunno per riflettere insieme su quanto accaduto e come rimediare, indirizzandoli anche, laddove necessario, allo sportello di ascolto; il referente del cyberbullismo ed il Dirigente scolastico dovranno essere sempre informati su quanto sta

accadendo e sulle azione intraprese. Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico come intervenire. Tali rilevazioni avvengono secondo i protocolli suggeriti dalla piattaforma messa a disposizione da "Generazioni Connesse". I docenti avranno anche a disposizione uno strumento di rilevazione delle criticità, sul quale descrivere le situazioni che si vengono a determinare, indicando anche le azioni messe in atto.

Le **azioni di prevenzione** di atti di bullismo e cyberbullismo messe in atto dalla scuola sono le seguenti:

- Organizzare eventi e/o dibattiti in momenti extrascolastici, rivolti a genitori, studenti e personale della scuola, sui temi della diversità e dell'inclusione.
- Organizzare eventi e/o dibattiti in momenti extrascolastici rivolti a docenti, studenti, genitori e personale A.T.A., di sensibilizzazione sui rischi che un uso non consapevole di Internet e delle tecnologie digitali può favorire.
- Organizzare incontri con esperti (tecnici informatici e Polizia Postale) dedicati alla prevenzione ed alla formazione per favorire, negli studenti, un utilizzo consapevole e controllato di internet e delle tecnologie digitali; tali incontri potranno essere estesi anche alle famiglie.
- Fornire ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori (es. liberatoria per la pubblicazione delle eventuali foto, immagini, testi e disegni relativi al proprio figlio).
- Non consentire l'utilizzo del cellulare personale degli alunni a scuola, in quanto per assolvere a ogni comunicazione urgente con i genitori o con chi ne fa le veci è sempre disponibile il telefono della scuola supervisionato dal personale addetto al centralino, che prima di passare la telefonata si accerta dell'identità dell'interlocutore.
- Consentire l'utilizzo del cellulare sono in casi particolari ed eccezionali, ad esempio quando ci si trova fuori dal contesto scolastico durante una visita guidata, e comunque sotto la supervisione del docente.
- Utilizzare filtri, software che impediscono il collegamento ai siti web per adulti (black list).

Le azioni di prevenzione sull'uso scorretto di Internet e delle nuove tecnologie rivolte ad alunni, genitori, docenti e personale ATA saranno incentrate su:

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 la componente studentesca: inserimento nel curriculum 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 la componente studentesca: inserimento nel curriculum 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 gli alunni e i 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 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.

<p>Violazione della privacy</p>	<p>Informazione sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farle rispettare.</p> <p>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.</p>
---------------------------------	---

PROGETTO GENERAZIONI CONNESSE
MODULO PER LA SEGNALAZIONE DI CASI

Nome di chi compila la segnalazione:

Ruolo:

Data:

Scuola:

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