Istituto Comprensivo
"S. G. Bosco-BenedettoXIII-Poggiorsini"
70024 Gravina in Puglia - Corso Vittorio Emanuele, 32/34
Tel. - Fax 080-322-1229
www.scuolasgboscogravina.it
baic88100c@istruzione.it baic88100c@pec.istruzione.it
c.f. 82014660722

ISTITUTO COMPRENSIVO "S.G. BOSCO - BENEDETTO XIII - POGGIORSINI" - -GRAVINA IN PUGLIA
Prot. 0001877 del 28/04/2018
03-05 (Uscita)

E-Safety Policy

a.s. 2017/2019
2019/2022

Approvato con delibera n° 13 del Collegio dei Docenti del 06/12/2019

CONTENUTI

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. Integrazione della *policy* con Regolamenti esistenti.

2. Formazione e Curricolo

2.1. Curricolo sulle competenze digitali per la componente studentesca.

2.2. Formazione del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.

2.3. Formazione del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

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

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

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

3.3. E-mail

3.4. Sito web della scuola

3.5. Social network

3.6. Protezione dei dati personali

4. Strumentazione personale/scolastica

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

4.2. Per il corpo docente e per il personale della scuola: gestione degli strumenti personali

4.3. Utilizzo del laboratorio di Informatica

5. Prevenzione, rilevazione e gestione dei casi

1. INTRODUZIONE

1.1. Scopo della policy.

Questa *policy* si applica a tutti i membri della comunità scolastica che hanno accesso o che sono utenti dei sistemi informatici della scuola.
In particolare, essa viene redatta per regolare il comportamento della componente studentesca dentro le aule scolastiche e per sensibilizzarli all'adozione di buone pratiche quando sono fuori dalla scuola e autorizza i membri del personale docente a erogare sanzioni disciplinari per comportamenti inappropriati avvenuti all'interno dell'Istituzione scolastica. Questo è il caso degli episodi di cyberbullismo come di altri fenomeni di cui si tratta nella presente politica, che possono avvenire al di fuori della scuola, ma che sono legati alla frequentazione della stessa.
L'Istituto comprensivo "S. G. Bosco-Benedetto XIII-Poggiorsini" accoglie minori "nativi digitali" che fin dall'infanzia sono esposti a rischi di cui sono inconsapevoli, pertanto la scuola attua parallelamente attività di prevenzione, controllo e formazione di allieve, allievi e famiglie allo scopo di ridurre al minimo l'occorrenza di atti che non solo creano disagio nella comunità scolastica, ma possono configurarsi come reati.
La scuola opera in stretto collegamento con le forze dell'ordine, con la Procura della Repubblica, con istituzioni del settore educativo, per mettere in campo strategie di prevenzione al cyberbullismo e interventi di recupero nel caso in cui vengano individuati tali fenomeni, informando i genitori/tutori e chiedendo la loro collaborazione anche qualora gli episodi si siano verificati al di fuori delle attività didattiche.

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 -entro la fine dell'a.s. 2017/18- all'attenzione del Consiglio di Istituto e del Collegio dei Docenti; valuta l'efficacia della politica e ne monitora/indirizza l'attuazione, anche in collaborazione con personale scolastico, enti locali e *stakeholder* territoriali. A tale scopo necessita di essere informato tempestivamente dal corpo docente e/o dal personale ATA sulle violazioni al presente regolamento, qualora se ne venga a conoscenza, o eventuali problemi attualmente non noti.

Animatore digitale e team dell'innovazione

Curano la redazione e la revisione annuale della policy sulla base delle osservazioni ricevute da tutti i soggetti interessati; ne assicurano la massima diffusione dentro la comunità scolastica in tutte le sue componenti (docenti/ata, genitori e studenti), mediante pubblicazione sul sito della scuola e sul blog dedicato all'innovazione digitale.
L'animatore, con il supporto del referente del laboratorio multimediale, si relaziona con la ditta che gestisce l'assistenza tecnico-informatica per definire le misure di sicurezza informatica più opportune; riferisce al Dirigente Scolastico situazioni o problemi di particolare rilevanza su cui intervenire.

Referente cyberbullismo

Coordina le iniziative di prevenzione e contrasto del cyberbullismo anche avvalendosi delle forze di polizia, nonché delle associazioni e dei centri di aggregazione giovanile presente sui territori.

Personale docente, con particolare riferimento ai Coordinatori dei Consigli di Classe

Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- garantire che gli alunni capiscano 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 esigenza di carattere informativo all'Animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola;
- 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 ATA

Il personale ATA è tenuto ad assicurare di:

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

Componente studentesca

Le alunne/gli alunni sono responsabili per l'utilizzo corretto dei sistemi informatici e della tecnologia digitale in accordo con i termini previsti da questa policy. In particolare sono tenuti a:

- non utilizzare dispositivi personali durante le attività didattiche, se non espressamente consentito dal personale docente;
- avere una buona comprensione delle possibilità di ricerca sul web e della necessità di evitare il plagio, rispettare le normative sul diritto d'autore, non diffondere dati personali;
- comprendere l'importanza della segnalazione di ogni abuso, uso improprio o accesso a materiali inappropriati e conoscere il protocollo per tali segnalazioni;
- conoscere e comprendere le politiche sull'uso di dispositivi mobili e di macchine fotografiche digitali;
- capire le politiche di utilizzo delle immagini ed essere consapevoli del significato e della gravità del cyberbullismo;

- capire l'importanza di adottare buone pratiche di sicurezza informatica in tutti i momenti della vita, a tutela dell'incolumità propria e altrui e per evitare di perpetrare reati punibili sia a livello scolastico sia da parte della magistratura;
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di Internet ai docenti e ai genitori.

Genitori

Genitori e tutori svolgono un ruolo cruciale nel garantire che i loro figli comprendano la necessità di utilizzare i dispositivi Internet e mobili in modo appropriato. La scuola coglierà ogni occasione per sensibilizzare i genitori circa questi problemi attraverso incontri con le autorità competenti ed altri esperti o educatori, circolari, sito web e altre comunicazioni telematiche, informazioni su campagne di sicurezza promosse da altre istituzioni o su convegni dedicati a questo tema. 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 delle aule;
- accesso alle sezioni del sito dedicate ai genitori, con particolare riguardo al registro elettronico;
- dispositivi personali dei loro figli nella scuola (dove ciò è consentito e/o autorizzato)

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:

- La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet sarà comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web e sul blog dedicato all'innovazione digitale;
- il personale docente sarà reso consapevole del fatto che il traffico in internet può essere monitorato e si potrà risalire al singolo utente registrato;
- un'adeguata informazione/formazione on-line del personale docente nell'uso sicuro e responsabile di internet, sia professionalmente che personalmente, sarà fornita a tutto il personale, anche attraverso il sito web della scuola;
- tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

Per la componente studentesca:

- Tutti gli alunni saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione;
- l'istruzione degli alunni riguardo all'uso responsabile e sicuro di internet precederà l'accesso alla rete;
- l'elenco delle regole per la sicurezza on-line sarà pubblicato in tutte le aule o laboratori con accesso a internet;
- sarà data particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili.

Per i genitori:

- La politica di e-safety sulla sicurezza nell'uso delle tecnologie digitali e di internet sarà resa pubblica nella sezione Regolamenti (https://www.scuolasgboscogravina.it/regolamenti.html) del sito web della scuola e nel registro elettronico;
- Sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di Internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali.

1.4. Gestione delle infrazioni alla Policy.

Disciplina degli alunni

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali di Internet di cui si dispone per la didattica, in relazione alla fascia di età considerate, sono prevedibilmente le seguenti:

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

Sono previsti pertanto da parte dei docenti provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento, quali:

- il richiamo verbale;
- il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività
- gratificante);
- il richiamo scritto con annotazione sul diario;
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente scolastico.

Disciplina del personale scolastico

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

- un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- una carente istruzione preventiva degli alunni sull'utilizzazione corretta e responsabile delle tecnologie digitali e di Internet;

- una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.

Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a Internet, la posta elettronica inviata/pervenuta a scuola, 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 Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

Disciplina dei genitori

In considerazione dell'età degli alunni e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico.

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

Monitoraggio dell'implementazione della Policy e suo aggiornamento.

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

1.5. Integrazione della policy con Regolamenti esistenti.

La presente policy è allegata in appendice al Regolamento di Istituto.

2. FORMAZIONE E CURRICOLO

2.1 Curricolo sulle competenze digitali per la componente studentesca.

La competenza digitale è ritenuta dall'Unione Europea una delle otto competenza chiave, per la sua importanza e pervasività nella società di oggi. L'educazione alla cittadinanza digitale è una necessità, non più un'opzione, è un dovere cui la scuola non può sottrarsi. Le abilità e le conoscenze che fanno capo alla competenza digitale sono trasversali a tutte le discipline e tutte concorrono a costruirla. Competenza digitale significa padroneggiare certamente le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con "autonomia e responsabilità" nel rispetto degli altri e sapendone prevenire ed evitare i pericoli. In questo senso, tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione.
Gli interventi formativi, progettati in verticale tra la scuola primaria e secondaria, con diverse gradazioni a seconda dell'età, sono finalizzati:

- utilizzare con dimestichezza le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall'attività di studio;
- essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, con particolare riferimento al contesto produttivo, culturale e sociale in cui vengono applicate.

2.2 Formazione del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

La formazione del corpo docente verrà organizzata su due livelli: interno ed esterno. A livello interno, nel PTOF si prevede che una parte della formazione in servizio obbligatoria ai sensi della L. 107/2015 sia dedicata proprio all'uso e all'inserimento delle TIC nella didattica e ai temi informatici in generale. Tale formazione è svolta da docenti dell'Istituto che fanno parte del team digitale, per cui il MIUR prevede opportuni percorsi la cui ricaduta viene annualmente tarata secondo le esigenze formulate dal Collegio Docenti, ed è improntata alla condivisione di esperienze significative e di buone pratiche.
Per quanto riguarda la formazione esterna, 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. Infine la scuola può aderire a progetti appositi di formazione presentati da enti e associazioni, come già avvenuto in passato.

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

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

L'accesso a internet è possibile e consentito per la didattica nei laboratori multimediali, ove vi è una postazione di lavoro per il docente (server) e postazioni in rete per gli alunni (client), e nelle aule dotate di L.I.M. e notebook ad esse collegate. Solo il docente dalla propria postazione può consentire agli alunni di accedere ad Internet. L'accesso è consentono solo a siti idonei alla didattica, secondo le impostazioni date dal responsabile di laboratorio che periodicamente provvede alla manutenzione e aggiornamento del sistema informatico e degli antivirus installati sui pc del laboratorio e, ove necessario, richiedendo l'intervento di tecnici esterni.
Occorre sensibilizzare tutta la comunità scolastica sull'opportunità di controllare i dispositivi di archiviazione esterna che vengano collegati al proprio pc.
Formare gli allievi all'uso di prodotti open source e fornire una maggiore protezione da infezioni di virus.

3.2 Gestione accessi.

L'Istituto attualmente è dotato di una rete wireless destinata all'utilizzo didattico da parte del corpo docente. La password è unica a livello di Istituto/plesso, ma la scuola sta valutando l'ipotesi di assegnare una password per ciascun utente allo scopo di monitorare meglio eventuali usi impropri e di estendere il servizio. Tale leva strategica è stata inserita nel PTOF.
In particolare l'Istituto intende mantenere un log corrente sull'uso dei sistemi della scuola per la verifica di eventuali violazioni della policy, oltre che delle leggi vigenti, da parte di chiunque abbia accesso a essi. Ciascun utente connesso alla rete dovrà: rispettare il presente regolamento e la legislazione vigente succitata, tutelare la propria privacy, quella degli altri utenti adulti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche

cui ha accesso e rispettare la cosiddetta netiquette (insieme di regole, comunemente accettate e seguite da quanti utilizzano Internet e i servizi di rete, che disciplinano il comportamento di un utente nel rapportarsi agli altri utenti attraverso risorse come wiki, newsgroup, mailing list, forum, blog o e-mail).
I genitori saranno invitati a firmare e restituire un modulo di consenso. La componente studentesca dovrà impegnarsi a rispettare le norme di buon utilizzo che la scuola si impegna a redigere e a divulgare prima che sia concesso l'accesso a Internet.

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 le cui credenziali sono in possesso del personale amministrativo. L'eventuale invio o ricevimento di posta a scopi didattici avverrebbe solo su autorizzazione del Dirigente scolastico e operativamente sarebbe svolto dall'assistente amministrativo addetto. La posta elettronica è protetta da antivirus, e quella certificata anche dall'antispam.

3.4 Sito web della scuola.

I dati di contatto sul sito web devono essere: indirizzo della scuola, e-mail e numero di telefono. Solo eccezionalmente, previa richiesta alla scuola, sono utilizzabili le comunicazioni via fax.
Il sito prevede un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali, avvisi di carattere generale, e un'area riservata accessibile solo dopo autenticazione.
Il personale che è in possesso delle credenziali per la gestione dei contenuti sul portale si assumerà la responsabilità editoriale di garantire che il contenuto inserito sia accurato e appropriato.

3.5 Social network.

Nella pratica didattica si cerca di educare la componente studentesca al loro uso sicuro. Per esempio a ogni utente sarà consigliato di non fornire mai dati personali di alcun tipo che possano identificare con
precisione le persone e la loro residenza o ubicazione.
La componente studentesca non deve pubblicare senza permesso foto personali proprie o altrui su qualsiasi spazio di social network previsto nella piattaforma di apprendimento scolastico.
Alunne/alunni, genitori e personale docente/ATA saranno informati sull'uso sicuro degli spazi di social network e sulle conseguenze legali di ogni uso improprio.
Alunne e alunni saranno invitati a usare nickname e avatar non riconoscibili quando utilizzano siti di social networking.

3.6 Registro elettronico.

Ogni famiglia riceve le credenziali per l'accesso riservato al registro elettronico, in cui il corpo docente è tenuto a registrare assenze, valutazioni, note e osservazioni. L'uso del registro elettronico è spiegato alle famiglie nel corso del primo consiglio di classe dell'anno scolastico e la pubblicazione delle informazioni attraverso tale strumento assolve l'obbligo di comunicare prontamente ed efficacemente ogni evento riguardante l'alunno/a. Coloro che non possono accedere a Internet e di conseguenza non possono consultare il registro elettronico sono pregati di darne segnalazione al coordinatore del consiglio di classe, che verificherà la trascrizione delle comunicazioni sul diario e la firma dei genitori.

3.7 Protezione dei dati personali.

Si fa riferimento a tutto quanto previsto dal Decreto legislativo 30 giugno 2003, n. 196 (c. d. Codice della Privacy). Tuttavia, si possono individuare al riguardo alcune linee guida di e-safety:

- ➢ il personale non deve condividere numeri di telefono personali o indirizzi di posta elettronica privati con la componente studentesca e con i genitori. Un telefono o una e-mail della scuola sarà fornito al personale cui è richiesto il contatto con la componente studentesca o con i genitori.
- ➢ Le fotografie o i video da pubblicare sul sito che includano allieve e allievi saranno selezionati con cura e non permetteranno a singoli di essere chiaramente identificati a meno che non si tratti di eventi particolari per cui le famiglie potranno concedere opportuna autorizzazione. La scuola cercherà di utilizzare fotografie o video di gruppo piuttosto che foto integrali di singoli.
- ➢ I nomi completi di alunne e alunni saranno evitati sul sito web come pure nei blog, forum e wiki, in particolare se in associazione con le loro fotografie.
- ➢ All'atto dell'iscrizione è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico di immagini e video delle/dei minori secondo i principi sopra indicati.
- ➢ Ogni caso particolare sarà preso in considerazione per stabilire l'opportunità di pubblicare dati personali e sarà presentata apposita richiesta circostanziata che varrà solo per lo specifico evento.

4. STRUMENTAZIONE PERSONALE

4.1 Per la componente studentesca.

I telefoni 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.

Nella scuola primaria si chiede alle famiglie di non lasciare tali dispositivi ad alunne e alunni; nella scuola secondaria di primo grado all'ingresso in aula, dopo l'appello, la componente studentesca deposita telefoni e altri dispositivi dentro un armadietto appositamente collocato in classe e/o sulla cattedra.

Gli studenti e le studentesse con disturbi specifici di apprendimento concorderanno, ove previsto dai Piani Didattici Personalizzati, le modalità di impiego di strumenti compensativi quali tablet e computer portatili e le modalità di custodia nell'armadietto della classe.

Giochi e console che possono avere accesso a Internet non filtrato, non sono consentiti. Saranno requisiti dal docente che ravvisa l'infrazione, depositati nella cassaforte della segreteria e consegnati al genitore/tutore convocato, che sarà contestualmente informato dell'eventuale sanzione disciplinare comminata al trasgressore.

Nel caso in cui debbano comunicare con la famiglia durante l'orario scolastico, alunne e alunni possono usare gratuitamente la linea fissa della scuola rivolgendosi a un operatore; 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.

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/ATA.

Il personale preferirà, quando ciò è possibile, l'impiego della strumentazione fornita dalla scuola rispetto a quella personale (portatili, pc fissi, …); le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali. Telefoni cellulari, tablet, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate e in presenza di autorizzazioni da parte dei genitori già depositate presso la segreteria.
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). L'uso improprio della rete è contestato al titolare delle credenziali con cui è avvenuta la comunicazione.
Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (chiavette usb, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.
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; - si assuma la responsabilità di segnalare prontamente eventuali malfunzionamenti o danneggiamenti al responsabile di laboratorio; - non salvi sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili e proponga agli alunni attività di ricerca di informazioni in rete fornendo opportunamente loro indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento.

4.3 UTILIZZO DEL LABORATORIO DI INFORMATICA

Disposizioni sull'uso del laboratorio

1. Le apparecchiature presenti nella scuola sono patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.
2. 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.
3. Quando un insegnante, da solo o in classe, usufruisce del laboratorio 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.
4. L'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante.
5. Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software.
6. Nei laboratori è vietato utilizzare CD personali o altri dispositivi se non dopo opportuno controllo con sistema di antivirus aggiornato.
7. All'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il locale in ordine e le macchine spente correttamente.
8. In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile del laboratorio.
9. 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.

Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

Disposizioni sull'uso dei software

1. I software installati sono ad esclusivo uso didattico.
2. In base alle leggi che regolano la distribuzione delle licenze, i prodotti software presenti in laboratorio non sono disponibili per il prestito individuale. Nei casi in cui lo fossero in base a precise norme contrattuali i docenti interessati, dopo aver concordato il prestito con il Responsabile di laboratorio, devono compilare l'apposito registro di consegna software custodito in laboratorio.
3. E' fatto divieto di usare software non conforme alle leggi sul copyright. E' cura dell'insegnante-utente di verificarne la conformità. Gli insegnanti possono installare nuovo software sui PC del laboratorio previa autorizzazione scritta del Responsabile di laboratorio. Si raccomanda, quindi, di verificare che il software installato rispetti le leggi sul copyright.
4. E' responsabilità degli insegnanti che chiedono al Responsabile di laboratorio di effettuare copie di cd/dvd per uso didattico, di assicurarsi che la copia non infranga le leggi sul copyright in vigore.

Accesso a Internet

1. 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;
2. Internet non può essere usato per scopi vietati dalla legislazione vigente;
3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet;
4. E' vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare da internet software non autorizzati, scaricare e installare software senza licenza.

Norme finali

Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

Le misure di prevenzione comprendono l'integrazione nel curricolo 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. La scuola si avvale della collaborazione di enti e associazioni 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.

L'Istituto Comprensivo "S. G. Bosco-Benedetto XIII-Poggiorsini" attiva inoltre uno sportello di ascolto al quale la componente studentesca si può rivolgere per avere consigli e sostegno psicologico anche relativamente alle tematiche del cyberbullismo.
La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti. A partire dalla corretta formazione e sensibilizzazione di tutti gli adulti coinvolti, docenti e personale ATA sono invitati a essere

confidenti e custodi, diretti o indiretti, di ciò che le ragazze e i ragazzi vivono: *si raccomanda di evitare ogni atteggiamento accusatorio o intimidatorio per riuscire a ricevere dai minori più fragili segnalazioni e confidenze circa situazioni problematiche vissute.*
I docenti, in particolare, sono chiamati a prevenire e vigilare su problematiche, rischi e pericoli che bambine, bambini e adolescenti possono vivere e affrontare ogni giorno. La gestione dei casi rilevati va differenziata a seconda della loro gravità e discussa a livello di Consiglio di Classe.
Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e come rimediare. Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico come intervenire.

PREVENZIONE, RILEVAZIONE E GESTIONE

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 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 la componente studentesca: 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 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.

IL DIRIGENTE SCOLASTICO

Lucia PALLUCCA