



Ministero dell'Istruzione, dell'Università e della Ricerca
 Istituto Comprensivo Statale "G. Falcone e P. Borsellino"
 Via G. Giolitti, 11 – 20022 Castano Primo (MI)
 Tel. 0331 880344 - Fax 0331 877311
 C.M. MIIC837002 - C.F. 93001830152
 e mail: segreteria@icscastano.gov.it - www.icscastano.gov.it

Regolamento TIC

e

contrasto al bullismo e cyberbullismo

Indice

Premessa	2
Destinatari e campi di applicazione	2
Modalità di comportamento all'interno dei laboratori di informatica	2
Modalità di utilizzo dei dispositivi informatici all'esterno delle aule di informatica	4
Utilizzo dei dispositivi personali per attività BYOD	7
Utilizzo dei dispositivi personali per uso non didattico	8
Utilizzo della piattaforma "Google Suite for Education"	8
Problemi connessi all'uso improprio della comunicazione digitale	10
Bullismo e Cyberbullismo	13

Premessa

L'utilizzo delle tecnologie per la comunicazione è ormai parte integrante del processo di insegnamento-apprendimento e per questo l'Istituto "Falcone e Borsellino" ha ritenuto necessario dotarsi di un Regolamento che suggerisca comportamenti corretti e stabilisca norme per un utilizzo consapevole della rete e degli strumenti a disposizione.

Il presente regolamento è stato redatto in base alle indicazioni contenute in

- Legge n. 71, "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo" del 29 maggio 2017
- Legge della Regione Lombardia "Disciplina degli interventi regionali in materia di prevenzione e contrasto al fenomeno del bullismo e cyberbullismo" del 7 febbraio 2017
- Linee di orientamento per la prevenzione e il contrasto del cyberbullismo aggiornate dal MIUR dell'ottobre 2017
- Policy di e-Safety in vigore nell'Istituto
- Regolamento generale per la protezione dei dati personali n. 2016/679 (General Data Protection Regulation o GDPR)

Destinatari e campi di applicazione

Il presente regolamento è rivolto a tutti gli utilizzatori delle strumentazioni informatiche di proprietà dell'istituto e della rete internet, oltre che dei dispositivi personali all'interno degli edifici scolastici.

Contiene indicazioni relative a:

- A. modalità di comportamento all'interno dei laboratori di informatica
- B. modalità di utilizzo dei dispositivi informatici all'esterno delle aule di informatica
- C. utilizzo dei dispositivi personali per attività BYOD
- D. utilizzo dei dispositivi personali per uso non didattico
- E. problemi connessi all'uso improprio della comunicazione digitale
- F. bullismo e cyberbullismo

Modalità di comportamento all'interno dei laboratori di informatica

I laboratori dell'Istituto sono patrimonio comune. Pertanto il rispetto e la tutela delle attrezzature sono condizioni indispensabili per il loro utilizzo e per garantirne l'efficienza. I laboratori informatici e le tecnologie didattiche informatiche e multimediali sono a disposizione di tutti i docenti e studenti dell'Istituto e possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.

Gli utilizzatori devono attenersi al regolamento interno.

Accesso ai laboratori

- L'ingresso degli alunni nei laboratori è consentito solo in presenza dell'insegnante

- Il docente accompagnatore è responsabile dell'uso didattico di hardware e software. Particolare attenzione deve essere posta nel controllo degli alunni che accedono alla navigazione su Internet
- L'accesso al laboratorio avviene prendendo in consegna le chiavi di accesso dal personale addetto e apponendo la firma sull'apposito registro.
- All'ingresso nel laboratorio, è opportuno accertarsi che tutte le attrezzature siano in ordine.
- In caso si riscontrino anomalie e/o malfunzionamenti
 - i docenti devono darne tempestiva comunicazione al responsabile dell'aula di informatica del plesso
 - il responsabile dell'aula di informatica effettua un primo tentativo di risoluzione del problema
 - se necessario procede alla segnalazione del guasto al responsabile del Pronto Soccorso Informatico attraverso il modulo online disponibile sul sito della scuola
 - il responsabile dell'aula di informatica è tenuto a dare comunicazione alla Segreteria tramite apposito modulo in caso di risoluzione del problema/mancato intervento del pronto soccorso informatico/persistenza del problema.
- Ove si riscontrassero mancanze di materiale, è opportuno segnalarle prontamente al responsabile dell'aula di informatica che procede ad effettuare la richiesta d'acquisto all'ufficio di segreteria secondo le modalità concordate.
- Per qualsiasi spostamento dei PC e di tutte le apparecchiature del laboratorio di informatica (tastiere, stampanti, mouse, casse audio etc.) è necessario riferirsi al responsabile dell'aula di informatica.
- È opportuno rispettare le procedure corrette di accensione, di utilizzo e di chiusura delle macchine (non togliere mai corrente fino a quando le macchine non hanno terminato la fase di spegnimento).
- Prima di utilizzare CD/DVD personali o altri dispositivi di memoria è necessario controllarli con antivirus e informare il responsabile d'aula.
- All'uscita dal laboratorio si deve lasciare tutto in ordine, i monitor, le stampanti e i computer spenti correttamente (chiudi sessione...); consegnare le chiavi del laboratorio al personale addetto e apporre la firma di uscita sull'apposito registro.

Utilizzo delle postazioni da parte dei docenti

I docenti che utilizzano laboratori e/o postazioni informatiche hanno l'obbligo di vigilare sul corretto utilizzo delle stesse da parte degli studenti sia quando operano singolarmente che in gruppo.

In particolar modo ogni docente è tenuto a:

- illustrare ai propri allievi le regole di utilizzo contenute nel presente documento;
- controllare che l'accesso degli alunni alla rete di Istituto avvenga sempre e solamente sotto la propria supervisione e unicamente con gli strumenti messi a disposizione dalla scuola, registrando opportunamente gli accessi alle singole postazioni (scuola secondaria);

- dare chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforma studenti ecc.), condividendo con gli alunni la *netiquette* e vigilando sul rispetto della stessa;
- assumersi la responsabilità della tracciabilità dell'utilizzo e del mantenimento in buono stato della strumentazione tecnologica da lui stesso e dagli alunni utilizzata, segnalando prontamente eventuali malfunzionamenti o danneggiamenti al Referente informatico;
- non divulgare le credenziali di accesso agli account (username e password) e/o, nel caso ne sia a conoscenza, alla rete wifi;
- non allontanarsi dalla postazione di classe, lasciandola incustodita;
- non salvare sulla memoria locale delle singole postazioni file contenenti dati personali e/o sensibili;
- proporre 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;
- lavorare solo su propri documenti facendo attenzione a non modificare quelli di altri utenti;
- alla fine di ogni seduta salvare il lavoro in cloud o su supporto rimovibile al fine di non occupare troppo spazio nell'hard-disk.

All'interno dell'aula multimediale non è consentito:

- consumare bevande o cibo
- cancellare software o dati presenti nel server o nei client;
- inserire software senza autorizzazione del responsabile: qualora si intenda installare programmi o scaricarli dai siti web, si potrà fare relativa segnalazione al responsabile che ne valuterà l'opportunità anche in base alla normativa sul diritto d'autore;
- modificare le configurazioni dei sistemi operativi e, in generale, qualunque impostazione dei pc (salvaschermo, sfondo, colori, suoni, pagina iniziale di Internet..);
- aggiungere cavi elettrici e collegamenti senza autorizzazione e, in ogni caso, trascurare le norme di sicurezza degli impianti.

Modalità di utilizzo dei dispositivi informatici all'esterno delle aule di informatica

Un uso adeguato dei pc portatili

- I portatili sono di proprietà della scuola e hanno un proprio numero identificativo e un numero di inventario. Ogni LIM è abbinata a uno specifico pc ed entrambi sono assegnati a un locale del plesso (e non alla classe).
- Tutti i docenti hanno il diritto di poter accedere singolarmente alle tecnologie informatiche per la preparazione delle lezioni e per le attività connesse all'attività di insegnamento, e con gli studenti per le attività didattiche.

- Se non sono disponibili gli armadietti a parete con serratura e chiave, i portatili devono essere custoditi nell'aula informatica/blindata o altro luogo concordato. I docenti della prima ora prelevano i dispositivi affidandoli ai colleghi che li seguono nell'orario giornaliero; alla fine delle lezioni il docente dell'ultima ora deve riportare il portatile in aula informatica/blindata o altro luogo concordato.
- I computer sono forniti di un sistema operativo e di applicazioni con licenza dell'Istituto o con licenza libera; qualsiasi software aggiuntivo, utile alla didattica, prima di essere installato deve essere autorizzato dal responsabile dell'aula di informatica del plesso, deve rispettare le leggi sul copyright ed essere compatibile con lo strumento.

Non è consentito

- consumare bevande o cibo in prossimità di apparecchiature
- portare i portatili della scuola al di fuori dell'edificio scolastico
- installare sul dispositivo applicazioni di natura illegale o di dubbia provenienza
- cedere il dispositivo a terzi (oltre a docenti e alunni), se non espressamente autorizzati dal responsabile di plesso dell'aula di informatica e/o dal Dirigente Scolastico.

Gli insegnanti

- sono responsabili dei portatili e hanno il compito di rendere gli alunni consapevoli dell'importanza della salvaguardia di un bene comune, seguendo le corrette norme di utilizzo
- non devono divulgare le credenziali di accesso agli account (username e password) e/o, nel caso ne sia a conoscenza, alla rete wifi
- utilizzano cartelle personali per salvare i propri lavori; è cura di chi provvede al corretto funzionamento delle macchine cancellare file di lavoro al di fuori delle cartelle personali
- non devono salvare file contenenti dati personali e/o sensibili nella memoria del portatile.

Il responsabile dell'aula di informatica del plesso

- si occupa della strumentazione: richieste di interventi di manutenzione, aggiornamento software, proposte di acquisti...
- fornisce supporto ai docenti
- deve segnalare al responsabile del Pronto Soccorso Informatico eventuali anomalie e/o malfunzionamenti riscontrati dai docenti attraverso il modulo online disponibile sul sito della scuola.

Gli alunni

- devono seguire le indicazioni dei docenti per il corretto utilizzo dello strumento
- sono tenuti a rispettare il regolamento.

Note operative per l'utilizzo della LIM e del pc portatile

Per mantenere un corretto funzionamento delle LIM in dotazione nelle classi si ricordano di seguito le modalità operative da seguire nell'utilizzo delle apparecchiature da parte di tutti i docenti:

A. Per accendere i dispositivi

5. inserire la spina dei dispositivi nella presa elettrica
6. accendere il videoproiettore utilizzando il telecomando schiacciando una sola volta il tasto di accensione
7. accendere il PC.

B. Per spegnere effettuare la procedura inversa

1. spegnere il computer come di consueto
2. spegnere il videoproiettore schiacciando una volta il tasto spegnimento del telecomando e una seconda volta lo stesso tasto dopo la richiesta di conferma che apparirà sulla LIM
3. aspettare che la spia luminosa del videoproiettore sia diventata fissa e che la ventola si sia fermata
4. togliere la spina dalla presa elettrica (e non limitarsi a premere il tasto della prolunga su "OFF")

C. I dispositivi mobili, utilizzati nelle attività in classe, dopo l'uso vanno riportati nell'aula informatica/blindata o altro luogo concordato insieme al mouse (se presente) e al cavo di alimentazione; in presenza di armadietto-custodia, riporre il portatile evitando di staccare i cavi dal computer in quanto spinotti e porte potrebbero danneggiarsi.

D. Riporre telecomando e penne nell'armadietto (o nel cassetto della cattedra) e chiuderlo prestando attenzione a non incastrarvi i fili.

E. Controllare che non si accumuli polvere negli angoli della LIM, luogo in cui sono allocati i sensori che permettono di far funzionare il touch.

F. Utilizzare le penne in dotazione ed evitare di rovinare la superficie della LIM, ad esempio utilizzando pennarelli colorati.

G. Non lasciare il computer acceso e incustodito a disposizione dei ragazzi.

H. L'utilizzo della LIM è consentito agli alunni esclusivamente per scopi didattici e sempre sotto la guida dei docenti.

I. Durante intervalli lunghi e alla fine dell'ultima ora spegnere il videoproiettore, onde evitare che la lampada si consumi inutilmente (ha un numero limitato di ore di funzionamento).

L. Il docente che dovesse riscontrare delle anomalie nel funzionamento di qualsiasi apparecchiatura, deve comunicarlo quanto prima al responsabile di plesso dell'aula di informatica per richiedere un intervento tempestivo di risoluzione del problema.

M. Non modificare le impostazioni del pc e della lavagna (password, account utente, salvaschermo, sfondo, colori, risoluzioni, suoni, pagina iniziale di internet ...).

N. È vietato l'uso della rete internet per scopi non legati alle attività didattiche; se possibile, si suggerisce il download di materiale funzionale alla lezione piuttosto che la consultazione online.

O. Eventuali lavori, creati dagli alunni o dagli insegnanti su altro dispositivo, devono essere acquisiti preferibilmente tramite cloud o supporti di memoria portatile previa autorizzazione del referente di plesso.

P. I file prodotti dagli alunni e dai docenti vanno salvati sul portatile in apposite cartelle dedicate.

Q. Entro la fine della scuola (mese di giugno) gli insegnanti devono provvedere a "fare pulizia" del materiale salvato, per permettere ai referenti di plesso di effettuare la formattazione dei computer.

Utilizzo dei dispositivi personali per attività BYOD (*Bring your own device*)

Ciascun docente aderisce volontariamente all'attività di BYOD, organizzandola nelle proprie classi, in un contesto di lavoro individuale o a gruppi, programmandola in accordo con gli altri docenti della classe.

Il docente, in accordo con le famiglie, stabilisce se il dispositivo personale portato da un alunno possa o meno essere utilizzato anche da altri alunni. Il lavoro in modalità BYOD può essere programmato a livello di classe, ma ciascun docente può discrezionalmente scegliere se attivare tale modalità nelle proprie ore o meno.

Ciascuna famiglia aderisce volontariamente all'attività di BYOD, dotando il proprio figlio di dispositivo e consentendogli di portarlo a scuola. Nessuna famiglia può essere costretta dalla scuola ad aderire o meno.

La scuola declina ogni responsabilità per furti o danneggiamenti occorsi ai dispositivi di proprietà degli alunni durante il periodo in cui non era in corso una lezione in modalità BYOD e, durante la lezione, se il danneggiamento è avvenuto a causa di un utilizzo improprio del dispositivo ad opera dell'allievo. Su richiesta dei genitori o per iniziativa del Consiglio di Classe o di Interclasse, è possibile istituire un armadio chiuso a chiave dove riporre i dispositivi degli allievi durante le ore della giornata. Nessun allievo può essere tuttavia costretto a riporre il proprio dispositivo in tale armadio e la scuola non è responsabile di furti di dispositivi ivi custoditi.

La scuola può attivare un sistema di password temporanee per il wi-fi, in modo da attivare il collegamento alla rete solo nei momenti previsti per la lezione. Un sistema di firewall renderà sicura la navigazione per gli allievi.

Byod può essere inteso anche come possibilità per i docenti di portare e utilizzare a scuola il proprio dispositivo personale a fini didattici. Nessun docente può essere obbligato a portare il proprio dispositivo e la scuola declina ogni responsabilità per furti o danneggiamenti al dispositivo di proprietà del docente.

Utilizzo dei dispositivi personali per uso non didattico

Durante l'orario scolastico agli alunni non è permesso l'utilizzo della telefonia mobile in nessuna funzione. La telefonia mobile di proprietà dello studente è concessa fuori dai locali scolastici e di pertinenza della scuola (cortile) salvo eventuali e specifiche autorizzazioni e salvo la modalità BYOD.

Utilizzo della piattaforma “Google Suite for Education”

Descrizione del servizio

- L'Istituto Comprensivo “G. Falcone e P. Borsellino” di Castano Primo (MI) mette a disposizione dei propri docenti, studenti e personale ATA la piattaforma “G Suite for Education” attivata come supporto alla didattica e alla gestione dell'Istituto.
- Il presente regolamento disciplina le condizioni di utilizzo del servizio di posta elettronica scolastica (in ambiente GMail) e delle applicazioni ad esso connesse; definisce anche le modalità di accesso per la fruizione del servizio.
- Il regolamento si applica a tutti gli utenti titolari di un account personale di istituto: docenti, studenti e personale ATA.e la sua accettazione è condizione necessaria per l'attivazione e l'utilizzo dell'account.
- Per gli studenti è indispensabile il consenso firmato dai genitori con il modulo 'Autorizzazione creazione account d'istituto' reperibile nella sezione Segreteria URP - Modulistica riservata - Progetti e corsi.
- Il servizio è fornito gratuitamente ed è fruibile fino al termine del percorso di studio degli studenti o al termine dell'attività lavorativa presso l'istituto dei dipendenti.
- Copia del regolamento è pubblicata sul sito web d'istituto www.icscastano.gov.it

Definizioni

Nel presente regolamento i termini qui sotto elencati hanno il seguente significato

- **Istituto:** Istituto Comprensivo “G. Falcone e P. Borsellino” di Castano Primo (MI)
- **Amministratore di sistema:** il responsabile incaricato dal Dirigente Scolastico per l'amministrazione del servizio.
- **Servizio:** servizio “Google Suite for Education”, messo a disposizione dalla scuola.
- **Fornitore:** Google Inc. con sede in 1600 Amphitheatre Parkway Mountain View, CA 94043.
- **Utente:** colui che utilizza un account del servizio.
- **Account:** insieme di funzionalità, applicativi, strumenti e contenuti attribuiti ad un nome utente con le credenziali di accesso.

Natura e finalità del servizio

Il servizio consiste nell'accesso agli applicativi di “Google Suite for Education” del fornitore.

- In particolare ogni utente avrà a disposizione una casella di posta elettronica, oltre alla possibilità di utilizzare i servizi aggiuntivi di *G Suite for Education* (Google Drive, Documenti Google, Google Moduli, Google Classroom, Sites, ecc.) senza la necessità di procedere ad alcuna installazione per la loro funzionalità sui PC, in quanto applicazioni Web Based.
- Il servizio è inteso come supporto alla didattica e ai servizi correlati con le attività scolastiche ingenerale: pertanto gli account creati devono essere usati esclusivamente per tali fini.

Soggetti che possono accedere al servizio in qualità di utenti

- a) Le credenziali per l'accesso saranno fornite dall'Amministratore di *G Suite* a docenti e personale ATA. a tempo determinato e indeterminato, che ne faranno richiesta e fino al termine dell'attività lavorativa presso l'Istituto.
- b) Gli studenti possono richiedere la creazione di un account, previa compilazione del modulo di consenso, che nel caso di minorenni deve essere firmato dai genitori. Il servizio sarà fruibile fino al termine del percorso di studi presso l'Istituto.
- c) Altre categorie di utenti possono richiedere la creazione di un account, sempre in relazione alle necessità didattiche o di servizio; in questo caso l'accoglimento della domanda è a insindacabile giudizio del responsabile Dirigente Scolastico.

Condizioni e norme di utilizzo

- Per tutti gli utenti l'attivazione del servizio è subordinata all'accettazione esplicita del presente Regolamento.
- L'utente può accedere direttamente al suo account istituzionale collegandosi a google.it, inserendo il suo nome utente: **cognome.nome@icscastano.edu.it** e la password fornita inizialmente dall'Amministratore e che sarà necessario modificare al primo accesso.
- Gli account fanno parte del dominio **www.icscastano.edu.it** di cui l'Istituto è proprietario.
- L'utente potrà cambiare in ogni momento la password di accesso. Nel caso di smarrimento l'utente potrà rivolgersi direttamente all'Amministratore della piattaforma.
- Ogni account è associato a una persona fisica ed è perciò strettamente personale. Le credenziali di accesso non possono, per nessun motivo, essere comunicate ad altre persone, né cedute a terzi in quanto come dettato dall'art. 24 del CAD (Codice dell'Amministrazione Digitale) sono equiparate all'uso della firma elettronica debole.
- L'Utente accetta pertanto di essere riconosciuto quale autore dei messaggi inviati dal suo account e di essere il ricevente dei messaggi spediti al suo account.
- L'utente s'impegna a utilizzare l'account esclusivamente per le finalità indicate al precedente Art.3b.
- L'utente s'impegna a non utilizzare il servizio per effettuare azioni e/o comunicazioni che arrechino danni o turbative alla rete o a terzi utenti o che violino le leggi e i regolamenti d'Istituto vigenti.
- L'utente s'impegna a rispettare le regole che disciplinano il comportamento nel rapportarsi con altri utenti e a non ledere i diritti e la dignità delle persone.
- L'utente s'impegna a non trasmettere o condividere informazioni che possano presentare forme o contenuti di carattere pornografico, osceno, blasfemo, diffamatorio o contrario all'ordine pubblico o alle leggi vigenti in materia civile, penale e amministrativa.
- È vietato immettere in rete materiale che violi diritti d'autore, o altri diritti di proprietà intellettuale o industriale o che costituisca concorrenza sleale.
- L'utente s'impegna a non procedere all'invio massivo di mail non richieste (spam).

- L'utente s'impegna a non divulgare messaggi di natura ripetitiva (cosiddette "catene di S. Antonio"), anche quando il contenuto sia volto a segnalare presunti o veri allarmi (esempio: segnalazioni di virus); a fronte di tale evenienza, l'utente è tenuto a segnalare all'Amministratore di piattaforma.
- L'utente s'impegna a non fare pubblicità, a non trasmettere o rendere disponibile attraverso il proprio account qualsiasi tipo di software, prodotto o servizio che violi il presente regolamento o la legge vigente.
- L'utente è responsabile delle azioni compiute tramite il suo account e pertanto esonera l'Istituto da ogni pretesa o azione che dovesse essere rivolta all'Istituto medesimo da qualunque soggetto, in conseguenza di un uso improprio.

Norme finali

1. In caso di violazione delle norme stabilite nel presente regolamento, l'Istituto nella persona del Dirigente Scolastico, potrà sospendere l'account dell'utente o revocarlo definitivamente senza alcun preavviso e senza alcun addebito a suo carico e fatta salva ogni altra azione di rivalsa nei confronti dei responsabili di dette violazioni.
2. L'Istituto si riserva la facoltà di segnalare alle autorità competenti - per gli opportuni accertamenti e i provvedimenti del caso - le eventuali violazioni alle condizioni di utilizzo indicate nel presente Regolamento, oltre che alle leggi e ai regolamenti vigenti.
3. L'account viene revocato:
 - a. immediatamente dopo reiterate violazioni del presente regolamento.
 - b. per gli studenti - dopo 90gg dal termine del percorso di studi presso l'Istituto
 - c. per i docenti assunti a tempo indeterminato e determinato (con termine incarico a giugno) - dopo 365 gg del rapporto lavorativo
 - d. nel caso di supplenze brevi - revoca dell'account dopo una settimana dal termine del contratto. Pertanto i suddetti utenti dovranno provvedere a scaricare e salvare dal proprio account i materiali e i file di interesse entro tale periodo.
4. L'Istituto s'impegna a tutelare i dati forniti dall'utente in applicazione del D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" e del D.Lgs. n. 101/2018 e successive modifiche e integrazioni, ai soli fini della creazione e mantenimento dell'account.
5. Il servizio è erogato dal fornitore che applica la propria politica alla gestione della privacy; l'utente può conoscere in dettaglio tale politica visitando il sito web del fornitore al link: <https://policies.google.com/privacy>

Problemi connessi all'uso improprio della comunicazione digitale

La comunicazione digitale è parte integrante della quotidianità di giovani e adulti, ma non per questo è priva di rischi e pericoli, soprattutto se di essa se ne fa un uso improprio, sia in maniera intenzionale che accidentale. Si ritiene quindi utile ricordare questi rischi in modo da prevenire inconvenienti o episodi spiacevoli e si ricorda che alcune condotte sono perseguibili in quanto reati, a partire dai 14 anni.

Reati e violazioni della legge

1. Al di là delle regole di buon senso ed educazione, vi sono comportamenti, talvolta solo

apparentemente innocui, che possono portare gli autori a commettere veri e propri reati e, di conseguenza, a subire procedimenti penali.

2. Quelli di seguito sono alcuni esempi di reati informatici (o che comunque possono essere posti in essere col mezzo informatico):

- Accesso abusivo ad un sistema informatico e telematico
- Diffusione di programmi (virus e malware) diretti a danneggiare o interrompere un sistema informatico
- Danneggiamento informatico
- Detenzione e diffusione abusiva di codici di accesso (password) a sistemi informatici o telematici
- Frode informatica
- Ingiuria
- Diffamazione a mezzo internet
- Sostituzione di persona
- Trattamento illecito dei dati personali
- Detenzione e diffusione di materiale pedopornografico
- Furto di identità
- Minacce e molestie.

Diritti d'autore (Copyright)

1. La legge 159/93 dispone, all'art. 1, che chiunque abusivamente riproduce a fini di lucro, con qualsiasi procedimento, la composizione grafica di opere o parti di opere letterarie, drammatiche, scientifiche, didattiche e musicali, che siano protette dalla legge ovvero, pone in commercio, detiene per la vendita o introduce a fini di lucro le copie, viola i diritti d'autore.

2. Esempi di questo tipo di violazioni si possono verificare

- quando una copia non autorizzata di un'opera digitale è caricata su un server e messa a disposizione degli utenti
- quando l'utente ottiene il documento, il software o il brano mp3 messo a disposizione in rete o acquistato e ne fa un uso illegittimo
- quando si opera la duplicazione abusiva di software proprietario a scopo di lucro o per un semplice fine di risparmio personale.

3. Qualora, a scopo di discussione, critica o informazione culturale, si volessero utilizzare parti di opere, brevi estratti o citazioni (mai l'opera integrale) nel realizzare lavori didattici o pagine web, si dovrà menzionare chiaramente il nome dell'autore e la fonte, per evitare infrazioni di copyright.

4. Le foto utilizzate non devono essere coperte da copyright e deve essere citata la LORO provenienza. Si raccomanda di cercare foto di libero utilizzo o libera modifica inserendo questi parametri nei filtri di ricerca.

5. Le musiche inserite nei filmati devono essere di libero utilizzo, se coperte da diritti SIAE questi devono essere pagati. Musiche di libero utilizzo sono disponibili in "JAMENDO".

Utilizzo di internet

Nell'uso di internet e della posta elettronica non sono consentite le seguenti attività:

- scaricare (download) software, applicazioni e file non necessari all'attività didattica o istituzionale
- farne un uso che possa in qualche modo recare qualsiasi danno all'Istituto o a terzi
- immettere in rete foto o filmati non autorizzati

- scaricare file che potrebbero essere protetti da diritti d'autore.

Osservanza delle disposizioni in materia di privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza. La diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere il soggetto in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati. Foto e riprese all'interno dell'istituto sono autorizzate solo a scopo didattico, la diffusione in rete di tali immagini e video, la loro condivisione sui social network e nei sistemi di messaggistica istantanea non è consentita, se non per lo stretto tempo necessario.

Sicurezza in rete

Per proteggere la propria privacy e la propria identità in rete è bene mettere in atto alcuni comportamenti "responsabili" quali

- utilizzare password sicure (almeno 8 caratteri comprendenti maiuscole, numeri e simboli) e diverse per ciascun sito/piattaforma
- non comunicare le proprie password ad altre persone
- non utilizzare i propri dati personali nelle password
- scegliere a quali applicazioni consentire l'utilizzo della geolocalizzazione
- controllare le impostazioni della privacy dei social network utilizzati, restringendo il più possibile l'accesso alle informazioni personali
- evitare di accettare le amicizie di persone che non si conoscono nella vita reale.

Sanzioni per il mancato rispetto del regolamento

INFRAZIONE	SANZIONE	ORGANO COMPETENTE A SOMMINISTRARE LA SANZIONE
A1 Usare il cellulare senza l'autorizzazione del docente	Consegna dell'oggetto al docente e riconsegna ai genitori da parte del Dirigente Scolastico	Docente
A2 Usare lo smartphone per elaborare immagini e suoni non attinenti con l'attività didattica e/o non autorizzate dal docente	Consegna dell'oggetto al docente e riconsegna ai genitori da parte del Dirigente Scolastico Sospensione dalle attività scolastiche fino a 3 giorni	Docente Consiglio di classe
B1 Comportamento verbalmente offensivo nei confronti di uno o più compagni esercitato singolarmente o in gruppo	Sospensione dalle lezioni fino a 5 giorni con allontanamento dalla scuola Esclusione dal viaggio di istruzione	Consiglio di classe

B2 Linguaggio aggressivo e offensivo esercitato tramite social network	Sospensione dalle lezioni fino a 10 giorni con allontanamento dalla scuola Esclusione dal viaggio di istruzione	Consiglio di classe
B3 Recidiva nei comportamenti di cui ai punti B1, B2,	Allontanamento dalla scuola per un periodo superiore a 15 giorni Esclusione dal viaggio di istruzione Allontanamento fino alla fine dell'anno scolastico Non ammissione allo scrutinio finale o all'esame di stato	Consiglio d'Istituto

Bullismo e cyberbullismo

Bullismo

“Un ragazzo è oggetto di bullismo, ovvero è prevaricato o vittimizzato, quando viene esposto, ripetutamente, nel corso del tempo, alle azioni offensive messe in atto da uno o più compagni.” (Olweus, 1968)

“Comportamento che mira deliberatamente a far del male o a danneggiare; spesso è persistente, talvolta dura settimane, mesi e persino anni ed è difficile difendersi per coloro che ne sono vittime.” (Sharp e Smith, 1995)

Negli episodi di bullismo possiamo riconoscere alcune caratteristiche ricorrenti

- asimmetria di potere tra bullo e vittima
- intenzionalità e premeditazione, non si tratta di azioni occasionali e casuali
- sistematicità, cioè reiterazione nel tempo
- molteplicità delle manifestazioni: dirette (aggressioni, violenze, furti, danneggiamenti...) o indirette (esclusione, isolamento, diffusione di false notizie,...)
- presenza di spettatori.

Nel concreto le azioni che possono essere definite “bullismo” sono prepotenze quali

- affermazioni spiacevoli o cattive da parte di un/a ragazzo/a o di un gruppo nei confronti di un altro ragazzo o ragazza;
- violenza fisica (colpi, pugni, calci ...)
- chiusura di un ragazzo o una ragazza in una stanza/aula/ripostiglio/armadio
- invio di biglietti contenenti offese, ingiurie o parolacce
- esclusione dal gruppo e mancato riconoscimento
- continue e ripetute prese in giro.

Alcune di queste condotte possono essere considerate azioni criminali e anti-sociali, quindi devono essere affrontate dalle autorità, mentre le condotte “non-criminali” devono essere

affrontate attraverso la collaborazione tra scuola e famiglie, con l'ausilio eventuale dei servizi presenti sul territorio.

Non rientrano nella definizione di bullismo invece, i seguenti comportamenti:

- litigi occasionali in cui si scontrano ragazzi senza che ci sia una differenza di forza tra i due;
- discussioni, anche accese, senza che ci sia prepotenza da parte di uno dei partecipanti.

Le figure coinvolte nei fenomeni di bullismo sono diverse, ma i protagonisti veri e propri sono due, il **bullo** e la **vittima**; è però importante ricordare che si tratta di un fenomeno di **gruppo**: l'85% degli episodi accade alla presenza di un gruppo di spettatori. Il bullo, spesso spalleggiato da un gruppo di gregari, si trova in una posizione di forza rispetto alla vittima, che spesso appare passiva, inerme e isolata. Il gruppo degli spettatori si può suddividere in 3 categorie: i sostenitori del bullo, i sostenitori della vittima e la maggioranza silenziosa.

Cyberbullismo

Secondo la legge 71/2017 con il termine *cyberbullismo* si intende "qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo."

Caratteristiche del cyberbullismo, comuni al bullismo, sono l'intenzionalità, la ripetitività e l'asimmetria di potere. La maggior parte delle vittime ha un'età compresa tra gli 11 e i 14 anni.

Le principali manifestazioni del cyberbullismo sono

Flaming: invio di messaggi deliberatamente ostili e opprimenti, inviati da un utente della comunità verso un altro individuo specifico

Sexting: derivato dalla fusione delle parole inglesi sex (sesso) e texting (inviare messaggi elettronici), indica l'invio di messaggi, testi e/o immagini sessualmente espliciti, principalmente tramite il telefono cellulare o tramite altri mezzi informatici

Sextortion: messaggi e immagini sessualmente esplicite a scopo di estorsione

Harassment: invio ripetuto e continuo di messaggi privati insultanti e volgari

Cyberstalking: molestie attraverso l'utilizzo di mezzi di comunicazione elettronica

Hate speech: pubblicazione sui social network o su piattaforme di comunicazione digitale di messaggi di insulto a sfondo razzista o di incitamento all'odio

Furto d'identità: violazione dell'account personale (social network, email o siti internet) di un'altra persona, spesso con lo scopo di inviare messaggi di insulto o per screditare la persona stessa

Exclusion: esclusione di un individuo da gruppi o chat di gruppo online

Happy slapping: aggressione o molestia reale filmata con supporti multimediali e in seguito condivisa con altri attraverso social network o sistemi di messaggistica.