

ALLEGATO N. 4

Procedure operative per la gestione delle infrazioni alla E-Safety Policy.

Ogni volta che un membro del personale o studente viola la E-Safety Policy, la decisione finale sul livello di sanzioni sarà a discrezione del Dirigente Scolastico e rifletterà le procedure comportamentali e disciplinari della scuola.

Di seguito sono fornite solo come esemplificazione:

STUDENTI:

INFRAZIONI	POSSIBILI SANZIONI
<ul style="list-style-type: none">• L'uso di siti non-educativi durante le lezioni.• L'utilizzo non autorizzato di e-mail.• L'uso non autorizzato del telefono cellulare (o altre nuove tecnologie) durante le lezioni.• Uso di instant messaging / siti di social networking.	Fare riferimento all'insegnante della classe/ E-Safety Coordinator/Dirigente Scolastico
<ul style="list-style-type: none">• L'uso continuato di siti non-educativi durante le lezioni dopo essere stato avvertito.• L'uso non autorizzato di e-mail dopo essere stato avvertito.• L'uso non autorizzato del telefono cellulare (o altre nuove tecnologie) dopo essere stato avvertito.• L'uso continuato messaggistica / chat room istantanea, siti di social networking, newsgroup.• L'uso di materiale offensivo.	Fare riferimento all'insegnante della classe/ E-Safety Coordinator/Dirigente Scolastico Escalation a: <ol style="list-style-type: none">1. rimozione dei diritti di accesso a Internet per un periodo;2. rimozione di telefono fino a fine giornata;3. contatto con i genitori.
<ul style="list-style-type: none">• Rovinare o distruggere deliberatamente i dati di qualcuno, violare la privacy altrui o messaggi inappropriati, video o immagini su un sito di social networking.• Invio di un messaggio e-mail o MSN che è considerato molestia o azione di bullismo.• Cercare di accedere a materiale offensivo o pornografico.	Fare riferimento all'insegnante della classe/ E-Safety Coordinator/Dirigente Scolastico Escalation a: <ol style="list-style-type: none">1. rimozione dei diritti di accesso a Internet per un periodo;2. rimozione del telefono fino a fine giornata;3. contatto con i genitori;4. contattare le autorità competenti.
<ul style="list-style-type: none">• Invio di e-mail o messaggi di MSN considerati molestia o bullismo dopo essere stato avvertito.• Accedere deliberatamente allo scaricamento o alla diffusione di qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofobico o violento.• Trasmissione di materiale che viola i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati.	Fare riferimento all'insegnante della classe / contatto con i genitori Altre possibili azioni di salvaguardia: <ol style="list-style-type: none">1. conservare le prove;2. informare i provider di servizi di posta elettronica del mittente;3. fare rapporto alle autorità competenti dove si sospetti la pedofilia o altre attività illegali.

- Portare il nome della scuola in discredito.

PERSONALE SCOLASTICO:

INFRAZIONI	POSSIBILI SANZIONI
<ul style="list-style-type: none"> • L'uso di Internet per attività personali non legate allo sviluppo professionale (shopping online, e-mail personali, instant messaging ecc.). • L'utilizzo di supporti di memorizzazione dei dati personali (ad esempio, chiavette USB) senza considerare l'accesso e l'adeguatezza di qualsiasi file memorizzato. • Non implementare adeguate procedure di salvaguardia. • Qualsiasi comportamento sul World Wide Web che compromette la professionalità del personale nella scuola e nella comunità. • L'uso improprio di primo livello di sicurezza dei dati, ad esempio uso illecito di password. • Violazione del copyright o della licenza per l'installazione di software . 	<p>Fare riferimento all' E-Safety Coordinator/DSGA /Dirigente Scolastico</p> <p>Escalation a:</p> <ol style="list-style-type: none"> 1. avvertimento
<ul style="list-style-type: none"> • Gravi danni intenzionali all'hardware o software del computer. • Qualsiasi tentativo deliberato di violare la protezione dei dati o di sicurezza informatica. • Creare, accedere, scaricare e diffondere deliberatamente qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofobico o violento. • Ricevere o trasmettere materiale che viola i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati. • Portare il nome della scuola in discredito 	<p>Fare riferimento all'E-Safety Coordinator/ DSGA /Dirigente Scolastico</p> <p>Altre azioni di salvaguardia:</p> <ol style="list-style-type: none"> 1. rimuovere il PC in un luogo sicuro per garantire che non vi è alcun ulteriore accesso al PC o laptop; 2. far verificare tutte le attrezzature per garantire che non vi è alcun rischio di alunni che accedono a materiali inappropriati nella scuola. <p>Escalation a: Contattare e fare rapporto alle autorità competenti</p>

Come saranno informati il personale e gli studenti di queste procedure?

- La E-Safety Policy sarà resa disponibile sul sito dell'Istituto a studenti, personale scolastico e genitori.
- I genitori firmeranno la E-Safety Policy quando il loro bambino inizierà la scuola.
- Agli studenti sarà insegnato un uso responsabile della rete in modo tale che possano sviluppare "comportamenti sicuri".
- Informazioni su come segnalare azioni di bullismo o cyber bullismo saranno messe a disposizione dalla scuola per gli alunni, il personale e i genitori.