



E-Safety Policy

Anno scolastico 2016-2017





Istituto Scolastico	Istituto Comprensivo “B. Grimaldi – L. Lombardi”- Bari
Policy creata in data:	aprile 2017
Data prevista per la revisione della Policy:	ottobre /novembre 2017
Gruppo di lavoro per la Policy:	Dirigente Scolastico Animatore digitale Membro del Team per l’innovazione digitale Referente del Progetto “Generazioni Connesse” Referenti d’istituto per le attività di prevenzione e contrasto al bullismo e cyber-bullismo
A partire dall’ a. s. 2017/2018	Rappresentanti dei genitori Alunni Tutor per ogni sezione della scuola secondaria

Il presente documento, redatto in base alle norme vigenti in tema di sicurezza e alle linee guida delle politiche nazionali ed è stato approvato dal Collegio dei Docenti in data 19 maggio 2017 (delibera n. 4) e dal Consiglio di Istituto in data 16 maggio 2017 (delibera n. 3)



Istituto Comprensivo
“B. GRIMALDI –L. LOMBARDI”
Via Lombardia, 2 - 70132 - BARI - Tel. e Fax 080/5371C.F.
93421950721 – E-MAIL: BAIC84300N@istruzione.it
www.icgrimaldilombardi.gov.it



INDICE DEGLI ARGOMENTI

- 1. INTRODUZIONE**
- 2. DOTAZIONE E UTILIZZO DI STRUMENTAZIONI MULTIMEDIALI DELLA
SCUOLA**
 - SPAZI A DISPOSIZIONE
 - STRUMENTAZIONE
- 3. STRATEGIE DI ATTUAZIONE DEL PIANO**
- 4. FORMAZIONE**
- 5. MODALITA' DI RILEVAZIONE E GESTIONE DEI CASI**
- 6. VADEMECUM PER LE FAMIGLIE SULL'USO SICURO DELLA RETE E DEI
DISPOSITIVI COMUNEMENTE USATI DAI RAGAZZI**



1. INTRODUZIONE

La presente Policy nasce con l’obiettivo di fornire uno strumento utile e di facile consultazione che consenta alla scuola e alle famiglie di gestire e prevenire casi problematici nati da un uso non corretto della tecnologia e dei dispositivi digitali utilizzati da bambini e ragazzi non sempre consapevolmente.

La Scuola è ubicata nel popoloso quartiere “San Paolo” di Bari, nato negli anni sessanta come quartiere di edilizia popolare; infatti, ancora oggi la zona è identificata con l’acronimo “CEP” - Comitato per l’Edilizia Popolare -.

Il quartiere, nel progetto iniziale, doveva essere autosufficiente, in grado di offrire tutti i servizi necessari ai residenti e adeguati collegamenti al centro della città.

L’assenza di efficienti servizi, purtroppo, ha relegato il quartiere ad una sorta di “periferia senza città”, nella quale si sono evidenziati fenomeni di disagio sociale e di devianza.

Nel corso degli ultimi decenni il quartiere è cresciuto a dismisura, ed è stato dotato di alcuni importanti servizi di pubblica utilità, quali l’ Ospedale, scuole di differente ordine, centri diurni di accoglienza per minori e famiglie in difficoltà, parrocchie, una palazzina per Uffici comunali, la sede dei Vigili Urbani e dei Carabinieri, la Cittadella della Polizia ed un’importante struttura di formazione della Guardia di Finanza.

Risultano, tuttavia, ancora carenti i servizi in prossimità dei nuovi insediamenti abitativi e permane un senso di insicurezza diffuso dovuto alla presenza di alcune sacche di emarginazione sociale, ragione per la quale la scuola rappresenta un veicolo fondamentale di legalità e buone pratiche a supporto delle famiglie.

Gli scopi del presente documento sono pertanto i seguenti:

- 1) **Proteggere** gli alunni attraverso la prevenzione.
- 2) **Garantire** agli alunni e alle famiglie un’efficace azione di supporto in caso di necessità.



- 3) **Dotare** la scuola di un regolamento chiaro ed efficace, che consenta l'utilizzo sicuro e consapevole della rete.
- 4) **Dotare** gli insegnanti di una procedura univoca ed efficace per gestire eventuali problematiche connesse all'uso della rete.
- 5) **Informare** i genitori e tutta la comunità scolastica sulle regole da condividere inerenti il tema in oggetto.
- 6) **Monitorare** il piano di azione registrando miglioramenti e lavorare periodicamente sulle eventuali criticità emerse.



2. DOTAZIONE E UTILIZZO DI STRUMENTAZIONI MULTIMEDIALI DELLA SCUOLA

L'Istituto si sviluppa su tre plessi scolastici. Numerosi sono i laboratori a disposizione per le varie discipline e attività. Nello specifico il Plesso Grimaldi possiede due piccoli laboratori con un totale di 17 postazioni computer e 9 classi dotate di Lim.

Il Plesso Lombardi possiede 3 laboratori dedicati all'utilizzo dei computer con oltre 40 postazioni e 8 classi dotate di Lim.

Gli altri laboratori sono dotati di proiettori.

Il Plesso Grimaldi è cablato con una connessione Lan mentre nel plesso Lombardi è presente la connessione Wi-fi.

Si segnala inoltre la presenza di una grande biblioteca - al momento poco utilizzata a causa della difficile gestione degli spazi - che l'Istituto intende valorizzare e utilizzare al meglio in futuro.



3. STRATEGIE DI ATTUAZIONE DEL PIANO

Il presente documento costituisce un aggiornamento della policy del Regolamento d'Istituto e riguarda: l'utilizzo dei laboratori, delle postazioni di lavoro e di Internet, l'utilizzo del telefono cellulare e dei vari dispositivi elettronici durante le attività scolastiche.

L'Istituto Grimaldi-Lombardi pertanto stabilisce le seguenti norme:

1. Ogni anno scolastico il Dirigente individua, in ciascun plesso, un Responsabile della Rete e dei laboratori di informatica.
2. Chi si propone come Responsabile delle aule multimediali, deve possedere conoscenze d'informatica atte ad assumersi tale responsabilità.
3. Gli allievi, gli esterni e il personale non preposto non possono accedere, né fisicamente né tramite computer, ai luoghi in cui sono custoditi dati e/o informazioni sensibili.
4. Il calendario delle lezioni che necessitano dell'utilizzo dei laboratori e delle postazioni d'informatica deve essere stabilito dagli incaricati della stesura dell'orario di ogni anno scolastico in coordinamento con il Responsabile.
5. L'accesso ai laboratori e/o alle postazioni di informatica in momenti diversi da quelli stabiliti nell'orario di cui al punto 4 deve essere autorizzato e concordato con la Presidenza e il Responsabile.
6. Quando si entra nel laboratorio, si deve accertare che tutto sia in ordine. Ove si riscontrassero malfunzionamenti o mancanze ci si dovrà riferire prontamente, senza manipolare nulla, al Responsabile che riferirà al DS.
7. La richiesta e il conseguente spostamento di apparecchiature multimediali in altro laboratorio o in aula deve essere richiesto con congruo anticipo al Dirigente.
8. Gli allievi devono sistemare gli zaini in zona del laboratorio che non impedisca un regolare sfollamento e non arrechi danno agli impianti, altrimenti devono lasciarli nelle classi.



9. Non è possibile cambiare di posto: tastiere, stampanti, mouse, casse o qualunque altra attrezzatura o stampato senza autorizzazione del Responsabile.
10. Il personale e gli allievi dovranno aver cura di rispettare le procedure corrette di accensione, utilizzo e di spegnimento delle macchine. Gli allievi non devono mangiare né ingerire liquidi nei laboratori.
11. È possibile l'utilizzo di CD o DVD, chiavi USB personali, solo previa autorizzazione del Responsabile e dopo controllo con antivirus.
12. Le stampanti devono essere utilizzate con accortezza e, comunque, secondo le regole stabilite dal regolamento interno ad ogni aula multimediale.
13. Prima di uscire dal laboratorio occorre accertarsi che le sedie siano al loro posto, che non vi siano cartacce o rifiuti e che tutte le apparecchiature elettriche siano spente.
14. Per motivi di manutenzione ordinaria e/o straordinaria, i PC possono essere riformattati senza alcun preavviso; si consiglia, pertanto, di salvare i dati in supporti di memoria esterni.
15. Periodicamente il Responsabile provvederà a controllare il funzionamento dei P.C.
16. Quando è stabilito per i PC è valido anche per le LIM.
17. La violazione del presente Regolamento potrà comportare la temporanea o permanente sospensione dell'accesso a Internet e/o alle risorse informatiche.
18. Falsificazioni e imbrogli non sono comportamenti approvati dall'Istituzione Scolastica.
19. È vietato cancellare o alterare file presenti in hard disk, installare o cancellare programmi, modificare le configurazioni dei PC in qualunque modo.
20. Gli utenti possono utilizzare le postazioni dell'Istituto per accedere a Internet solo per scopi didattici o collegati alle attività di lavoro degli uffici.
21. I software installati sono a esclusivo uso didattico o lavorativo. Chiunque abbia bisogno di aggiornamenti o nuovi applicativi da acquistare deve farne richiesta al Responsabile che riferirà al Dirigente.
22. Non è possibile fare copie del software presente nelle postazioni.



23. L'elenco dei software di cui la scuola possiede licenza è presente in Presidenza.
24. Si richiama l'osservanza delle norme per il rispetto del diritto d'autore e del copyright.
25. È vietato adottare comportamenti che possano interferire con la privacy, la policy e con la libertà di espressione.
26. Sono previste protezioni per impedire l'accesso a siti proibiti, software di sorveglianza continua e di blocco del sistema contro modifiche illecite.
27. È vietato tentare di alterare la propria identità di rete o tentare di impedire la propria identificazione e utilizzare le postazioni per arrecare molestie.
28. In rete occorre sempre rispettare tutti i vincoli di legge.
29. Comportamenti palesemente scorretti da parte degli utenti, quali violare la sicurezza di archivi e computer della rete, danneggiare le apparecchiature in qualsiasi modo, costituiscono dei veri e propri crimini elettronici e come tali sono punibili dalla legge.
30. I docenti Responsabili discuteranno con i colleghi e gli allievi della policy scolastica e degli eventuali problemi che possono verificarsi nell'applicazione delle regole concernenti l'uso di internet e i pericoli del web.

ACCOUNT

31. Gli utenti che otterranno un account per l'ingresso nella rete d'Istituto dovranno prendere visione del presente Regolamento e di quello eventualmente affisso in aula.
32. Il personale dell'Istituto, può richiedere di connettersi alla rete WI-FI locale dell'Istituzione Scolastica. La connessione è possibile previa informazione del Responsabile e autorizzazione del DS, che ne forniranno la chiave d'accesso.
33. Per la connessione temporanea di macchine di visitatori si fa riferimento al punto precedente.

INTERNET

34. Ogni plesso deve essere dotato di una password per i computer e di password WI-FI, laddove esistente, che il Responsabile comunicherà ai docenti interessati.



35. L'utilizzo di Internet è disciplinato tramite questo regolamento e le note affisse nelle aule multimediali; per quanto non specificato nel presente regolamento ci si attiene alle leggi previste per il campo dell'informatica. Il servizio è comunque da utilizzare per soli scopi didattici e di ricerca, da dettagliare e giustificare a richiesta del Responsabile o del DS.

36. Nel caso di invii di mail a gruppi di destinatari si devono evitare liste di distribuzione con indirizzi visibili per questione di privacy.

37. Non aprire file provenienti da fonti sconosciute; in particolare quelli con estensione ex, bat; riferirsi sempre al Responsabile

38. Prima di scaricare documenti e file, da internet chiedere al docente Responsabile.

39. Chiedere sempre il permesso prima di iscriversi a concorsi, e prima di riferire l'indirizzo della scuola.

40. È vietato sottoscrivere e/o accedere a newsletter, chat room, o social network, se non a quelli scolastici laddove presenti.

41. Il docente d'aula curerà e registrerà gli accessi all'aula informatica e a Internet, darà chiare indicazioni su come utilizzare il web, informando sui pericoli di internet. Tutte le navigazioni saranno monitorate.

POSTA

42. La posta sarà scaricata solo dal Responsabile dell'aula informatica, avendo cura di eliminare mail sospette e bloccare lo spam direttamente dal server web di riferimento.

43. È severamente vietato iscriversi, o lasciare i propri dati, o quelli della scuola a siti web, per non creare liste di spam nelle caselle di posta, aumentando la probabilità d'infezioni.

44. Gli unici siti ai quali si è abilitati sono quello d'Istituto e quelli strettamente connessi alla funzione docente, previo permesso chiesto al DS.



45. Le uniche mail abilitate all'apertura sono esclusivamente quelle inviate dalla Direzione o dalle scuole della presidenza dell'I.C., oppure quelle strettamente connesse a enti con i quali la scuola ha rapporti di rete.

46. Le regole del punto precedentemente sono valide anche per l'invio di posta.

47. Nel caso d'invii di mail a gruppi di destinatari si devono evitare liste di distribuzione con indirizzi visibili per questioni di privacy.

SITO WEB D'ISTITUTO

48. l'unico sottoscrittore di contratti con gestori di servizio è il Dirigente Scolastico, come legale rappresentante dell'Istituto.

49. Lo sviluppo del sito scolastico è affidato a una figura specifica, designata dal dirigente.

50. È responsabilità di suddetta figura, garantire che il contenuto e la struttura del sito sia accurato e appropriato.

51. Il sito scolastico è dotato di albo pretorio con valore legale, le pubblicazioni effettuate solo su carta non hanno più questo valore, (art. 32 della Legge n. 69/2009).

52. La scuola detiene i diritti d'autore dei documenti che si trovano sul sito, oppure chiede il permesso per pubblicare documenti su cui gravano i diritti d'autore.

53. La scuola può inserire, a scopo di critica, di discussione, d'informazione culturale, parti di opere, brevi estratti o citazioni, menzionando il nome dell'autore o la fonte (L. 2/4/1941 n°633, art.70).

54. In via eccezionale, è possibile richiedere la pubblicazione sul sito di rubriche o pagine, solo se già elaborate dal richiedente in file: la richiesta sarà vagliata dal Referente del sito web ed autorizzata dal DS:

55. Il referente del sito web dell'istituzione scolastica ne assicura l'aggiornamento periodico.



56. La pubblicazione in rete di foto degli allievi è possibile previa acquisizione di liberatoria da parte dei genitori, in caso contrario si sfoccheranno, con software di ritocco fotografico, i volti.

57. Per eventuali recapiti e informazioni, saranno dati l'indirizzo e i numeri di telefono della scuola, mentre non sarà pubblicato alcun recapito privato del personale della scuola.

58. In calce al sito, sono indicati gli indirizzi, tramite i quali è possibile contattare il DS e il Responsabile, mentre tutti i dati generici dell'I.C. si trovano in home page.

59. L'utilizzo del Sito, la consultazione dei dati in esso contenuti e l'impiego dei servizi attivati costituisce accettazione dell'informativa sulla privacy nel web, delle Note Legali e delle loro possibili future revisioni: rileggere quindi di frequente questi documenti.

60. L'Istituto si riserva il diritto di rifiutare o revocare l'accesso al Sito e/o ai servizi offerti senza preavviso agli utenti che forniscono informazioni errate, non interpretabili, o che non rispettino i termini e le condizioni di utilizzo previsti nelle Note Legali.

61. Gli utenti che otterranno un account per l'ingresso nel sito web d'Istituto dovranno prendere visione del presente Regolamento e di tutte le norme di legge e attenervisi.

62. Il sito web è conforme alle normative per i siti delle pubbliche amministrazioni, continuamente aggiornato a fronte dello sviluppo di nuove tecnologie web e delle norme emanate in merito.

63. Sul sito dell'I.C. nei link in calce a tutte le pagine, si trovano i riferimenti di legge riguardo a privacy nel web, policy web, trasparenza, pubblicità legale (Albo Pretorio), accessibilità. Si prega di leggere molto attentamente e guardare spesso tali documenti, perché essi sono aggiornati periodicamente a seguito delle normative attinenti.

UTILIZZO DI STRUMENTAZIONE PERSONALE

64. Non è consentito agli studenti l'uso di telefoni cellulari all'interno dei locali scolastici a meno di autorizzazione da parte di un docente.



65. È fatto esplicito divieto, comunque, di diffondere immagini, video o dati di qualsiasi natura relativi alla vita scolastica senza aver preventivamente informato le persone coinvolte e averne ottenuto il consenso.

66. La scuola si riserva di individuare le opportune modalità di custodia dei telefoni cellulari che gli alunni dovessero portare con sé.

67. Nel caso in cui gli alunni portassero a scuola PC portatili, tablet, notebook o altre strumentazioni personali, gli alunni ne saranno personalmente responsabili e nessun danno eventuale potrà essere addebitato alla scuola stessa

68. I docenti utilizzeranno i telefoni cellulari per ragioni legate alla didattica e, per ragioni personali, solo in caso di effettiva necessità.

69. La norma 68 è valida per tutto il personale della scuola

Il personale della scuola si impegna a rispettare le suddette norme.

L'Istituto si impegna a valorizzare nel Curricolo le competenze digitali degli studenti con particolare attenzione a far loro acquisire consapevolezza delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, in riferimento soprattutto al contesto produttivo, culturale e sociale in cui vengono applicate.

Si impegna, altresì, a favorire la formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica e sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali così come previsto dal Piano Nazionale Scuola Digitale e dal Piano di attuazione dello stesso.

L'Istituto continuerà ad attivare costantemente iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine continueranno gli incontri fra docenti e genitori e con i rappresentanti delle forze dell'ordine e associazioni per la sensibilizzazione e per la diffusione di materiale informativo sulle tematiche trattate. Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con



Istituto Comprensivo
“B. GRIMALDI –L. LOMBARDI”
Via Lombardia, 2 - 70132 - BARI - Tel. e Fax 080/5371 C.F.
93421950721 – E-MAIL: BAIC84300N@istruzione.it
www.icgrimaldilombardi.gov.it



l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo.

La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento (Policy e-safety) per portarle a conoscenza delle famiglie.



4. LA FORMAZIONE DEI DOCENTI

Sulla scorta delle direttive ministeriali della didattica per competenze, l'I.C. Grimaldi Lombardi ha, da tempo, individuato come priorità la formazione dei docenti, diretta a fornire loro gli strumenti necessari ad aiutare gli alunni non solo a riconoscere e ricordare fatti e strutture, ma a scomporli, confrontarli e, infine, utilizzarli per produrre qualcosa di nuovo e interessante (secondo il livello più elevato della tassonomia di Bloom).

Muovendo dalla convinzione che ogni alunno abbia dei bisogni educativi individuali, la scuola ha come obiettivo quello di favorire la formazione dei docenti in modo che essi possano essere veicoli di apprendimento per tutti gli alunni, utilizzando ogni strumento che la moderna metodologia didattica mette a disposizione.

Tali strumenti, infatti, più della didattica tradizionale, attraverso la collaborazione e lo sviluppo delle competenze - non solo disciplinari ma sociali e civiche - possono favorire la crescita del bambino e del ragazzo come alunno e, soprattutto, come persona.

Un occhio particolarmente attento è rivolto, pertanto, alla formazione nell'uso delle competenze digitali, strumento ormai irrinunciabile in qualsiasi settore del vivere comune e, quindi, anche nella scuola.

Nella convinzione, pertanto, che l'utilizzo delle TIC possa contribuire al conseguimento delle competenze disciplinari e trasversali, diversi docenti si stanno formando per utilizzare sempre più proficuamente le varie tipologie di didattica innovativa, quali piattaforme di *Social Learning*, *Flipped Classroom*, *Coding*, *Robotica educativa*.

Consapevoli che l'integrazione delle TIC e di internet nella scuola richiedono una conoscenza approfondita anche dei rischi che la rete comporta, si sta procedendo a formare i docenti stessi anche nel campo dei fenomeni legati all'uso improprio delle nuove tecnologie, con particolare riferimento alle dinamiche socio-comunicative legate alla comunicazione in rete.

Nel corso del prossimo anno scolastico proseguirà il percorso formativo - già avviata nel presente anno dal Comune di Bari in sinergia con l'Università degli Studi “Aldo Moro” - su tale tema, denominato “Reputazione in rete”.



Detto percorso formativo, che è rivolto nella sua fase iniziale a docenti referenti, sarà, successivamente, esteso a tutti i docenti e agli alunni della scuola, nonché alle famiglie. Proseguiranno anche i corsi dedicati agli insegnanti e al personale di segreteria nell'ambito del Piano Nazionale Scuola Digitale.

Sempre nell'ambito della formazione rivolta all'uso consapevole della rete, si tengono, ormai da diversi anni, incontri con la Polizia Postale, rivolti a docenti, alunni e genitori.

5. MODALITA' DI RILEVAZIONE E GESTIONE DEI CASI

Premessa:

Da sempre l'I.C. “Grimaldi- Lombardi” coltiva l'idea che un apprendimento significativo possa realizzarsi solo nel luogo in cui i bambini, prima, e i ragazzi, poi, si sentano accolti e riconosciuti con le proprie peculiarità e i propri modi di essere.

L'insegnante, pertanto, facendo leva sull'innato bisogno di relazioni umane, dovrà badare a creare con gli alunni e fra gli alunni una relazione di ascolto e di conoscenza reciproca, atta a favorire comportamenti corretti e significativi e prevenire, al contempo, atti di prevaricazione e di esclusione.

Verranno, altresì, sistematicamente adottati progetti e strategie, con l'obiettivo di prevenire episodi di bullismo e cyber bullismo, atte a coinvolgere i ragazzi, inducendoli al confronto e al dialogo, impostando con loro un rapporto di fiducia e di condivisione. Se, tuttavia, si presentassero casi di comportamenti quali bullismo, cyberbullismo, adescamento, sexting, happy-slapping, outing..., il comportamento che il docente dovrà adottare è il seguente:

- 1) cercare di dialogare con l'alunno in difficoltà per comprendere al meglio la situazione
- 2) deresponsabilizzare la vittima, che spesso si colpevolizza per l'accaduto
- 3) informare della situazione il C.d.C., il Dirigente e il responsabile della e-safety
- 4) indurre il ragazzo al dialogo con la famiglia



- 5) far rimuovere tempestivamente gli eventuali contenuti on line lesivi della persona colpita, segnalandoli a Generazioni Connesse (“clicca e segnala” o “stop it”)
- 6) fornire alla famiglia della vittima le opportune informazioni per la migliore risoluzione della problematica (metterla in contatto con la Help Line di *Generazioni Connesse* 1.96.96)
- 7) nei casi ritenuti gravi, allertare le autorità competenti affinché intercettino il colpevole degli atti persecutori.

6. VADEMECUM PER LE FAMIGLIE SULL’USO SICURO DELLA RETE E DEI DISPOSITIVI COMUNEMENTE USATI DAI RAGAZZI

Consigli generali

- Cercate di utilizzare il tablet, lo smartphone o il computer insieme ai più piccoli: in modo da educarli ad un uso corretto di questi strumenti. Ricordate che non sono giocattoli.
- Molte chat o social network richiedono un’età minima (13 o 18 anni): non permettete ai vostri figli che si iscrivano fornendo false informazioni riguardo all’ età. Rimanete vicino a loro mentre creano profili e insegnate ai vostri figli, soprattutto ai più piccoli, l’importanza di non rivelare in Rete la loro identità. Spiegategli che è importante per la loro sicurezza e per quella di tutta la famiglia non fornire dati personali (nome, cognome, età, indirizzo, numero di telefono, nome e orari della scuola, nome degli amici ecc.) che potrebbero essere usati da adulti malintenzionati o da potenziali pedofili.
- Spiegate ai vostri figli che è illegale creare dei profili sui social network con nomi di altre persone: è un furto di identità!
- Spiegate ai vostri figli come navigare sicuri anche se vostro figlio non sembra interessato a Internet. Infatti in qualsiasi momento, fuori da casa (a scuola, a casa di un amico, in un internet caffè, ecc...) potrebbe essere incuriosito e avere voglia di navigare sulla Rete. Per questo motivo è bene che sia al corrente di quali semplici e importanti regole deve seguire per essere sicuro e protetto mentre si diverte.
- Controllate i più piccoli guidandoli nella navigazione per conoscere i loro interessi e poter dare consigli sui siti da evitare e su quelli da visitare.



- Non posizionate il computer nella camera dei ragazzi ma scegliete una stanza centrale della casa accessibile a tutta la famiglia, in modo da poter dare anche solo una fugace occhiata ai siti visitati senza che vostro figlio si senta “sotto controllo”.
- Impostate la “cronologia” in modo che mantenga traccia per qualche giorno dei siti visitati da vostro figlio e controllatela periodicamente. Effettuate anche un controllo del contenuto dell’hard disk del computer
- Aumentate il filtro del “parental control” attraverso la sezione sicurezza in Internet” dal pannello di controllo.
- Usate software “filtri” con un elenco predefinito di siti da evitare. Verificate periodicamente che funzionino correttamente e tenete segreta la password.
- Insegnate ai vostri figli preadolescenti e adolescenti a non accettare mai di incontrarsi personalmente, magari di nascosto, con chi hanno conosciuto in Rete. Spiegate come un computer collegato a Internet sia per alcune persone male intenzionate il modo migliore per nascondere propositi criminali dietro bugie e false identità, a volte molto attraenti.
- Leggete sempre le e-mail con i bambini più piccoli controllando ogni allegato al messaggio. Se non conoscete il mittente non aprite l’e-mail, né eventuali allegati: possono contenere virus, troiani o spyware in grado di alterare il funzionamento del vostro computer. Date le stesse indicazioni ai ragazzi più grandi.
- Non aprite gli allegati delle e-mail provenienti da sconosciuti e verificate prima il nome dei mittenti e l’oggetto.
- Siate sospettosi anche di allegati inaspettati ricevuti da chi conoscete perché possono essere spediti da una macchina infettata senza che l’utente ne sia a conoscenza.
- Installate un buon antivirus e un firewall che proteggano continuamente il vostro pc e chi lo utilizza. I Firewall sono essenziali per chi ha una connessione ADSL o via cavo, ma sono preziosi anche per chi utilizza la connessione telefonica. Aggiornate e scaricate le nuove versioni dei programmi per avere la garanzia di una protezione continua del computer.
- Dite ai bambini di non rispondere quando ricevono messaggi di posta elettronica, , su Whatsapp, su Facebook o attraverso altre chat, di tipo volgare, offensivo e, allo stesso tempo, invitarli a non usare un linguaggio scurrile o inappropriato e a comportarsi correttamente in rete.
- Spiegate ai bambini che può essere pericoloso compilare moduli on line o effettuare registrazioni su siti web sconosciuti e dite loro di farlo solo dopo avervi consultato. Aiutateli a proteggere i loro account password complesse (composte da lettere, numeri, maiuscole, minuscole, segni di interpunzione, simboli...)
- Non lasciate troppe ore i bambini e i ragazzi da soli in Rete. Stabilite delle regole fisse su quanto tempo possono passare navigando su Internet: limitare il tempo che possono



trascorrere on-line significa limitare di fatto l'esposizione ai rischi della Rete. Siate costanti nel fare rispettare le regole.

- Usate software "filtri" con un elenco predefinito di siti da evitare. È opportuno però verificare periodicamente che funzionino in modo corretto e tenere segreta la parola chiave
- Stabilite quanto tempo possono passare navigando su Internet. Un uso eccessivo e senza controllo potrebbe causare ai vostri figli una forma grave di dipendenza.
- Non consentite ai vostri figli di usare la vostra carta di credito senza il vostro permesso o di comprare oggetti on line. Non consentite loro di scaricare programmi o video o musica in violazione del diritto d'autore

Consigli sull' uso sicuro del telefonino da parte dei minori

- Spiegate a vostro figlio che il telefonino è un mezzo di comunicazione e deve essere usato con la stessa cautela che si ha nei confronti del computer. Scegliete per i più piccoli modelli semplici e rimandate l'acquisto di quelli con telecamera e fotocamera a quando saranno in grado di utilizzarli in modo sicuro e consapevole.
- Spiegate a vostro figlio che foto e riprese effettuate con il telefonino sottostanno alla normativa italiana in materia di protezione dell'immagine e della privacy delle persone.
- Spiegate a vostro figlio che in community e chat, si corrono rischi in termini di adescamenti da parte di pedofili on-line.
- Scegliete per i vostri figli SIM Card ricaricabili e ricaricate sempre voi il credito in modo da poter monitorare la quantità di traffico telefonico effettuato.
- Al momento dell'attivazione della SIM Card fornite ai vostri figli il PIN ma non il PUK. Con il PUK infatti potrete accedere al telefono anche se il PIN è stato modificato.
- Spiegate ai vostri figli che sms o mms che promettono ricariche facili o altri vantaggi immotivati sono spesso il primo contatto effettuato da chi non ha buone intenzioni.
- Spiegate ai vostri figli i pericoli che si corrono nel richiamare con il telefono numeri sconosciuti da cui provengono squilli o chiamate mute.
- Spiegate quali sono i rischi che si corrono nel diffondere foto o filmati con il



telefonino su social network o chat telefoniche. Una volta immesse in Rete foto e filmati , possono continuare ad essere diffuse senza controllo; inoltre aumenta il pericolo che le foto vengano viste o utilizzate in maniera impropria da pedofili.

Comportamenti allarme

I motivi per cui vostro figlio assume particolari comportamenti possono essere molteplici e non tutti vanno sempre ascritti a situazioni di abuso o molestie.

Potrebbe essere tutt'altra l'origine del turbamento di vostro figlio, soprattutto se sta attraversando un momento evolutivo particolare (preadolescenza, adolescenza, separazioni o cambiamenti familiari). Tuttavia, se questi comportamenti riguardano l'uso del computer o del telefonino, vale la pena cercare di comprendere cosa sta realmente accadendo.

Ecco i casi in cui prestare attenzione:

- se tuo figlio modifica improvvisamente l'uso del telefonino o del computer e passa molto tempo a scrivere sms, a effettuare o ricevere chiamate, anche in tarda serata, e rimane connesso per molte ore al PC;
- quando si allontana e si apparta ogni volta che riceve o effettua una chiamata con il telefonino o si connette a Internet;
- se mostra ansia o rifiuta categoricamente di farti vedere il suo telefonino o lo schermo del computer mentre naviga o è connesso;
- se consuma molto velocemente il credito telefonico e non ti dà spiegazioni circa i suoi consumi;
- se mostra ansia e preoccupazione quando squilla il telefonino o mentre è connesso senza spiegarne spontaneamente il perché;
- quando modifica i ritmi sonno-veglia (dorme troppo, dorme poco, ha incubi) o il comportamento alimentare e il rendimento scolastico.



Glossario

ADWARE: Software scaricato, spesso in maniera inconsapevole, durante la navigazione in Internet o l'installazione di un software gratuito, programmato per raccogliere informazioni sulle operazioni effettuate dall'utente e per visualizzare periodicamente messaggi pubblicitari non richiesti.

ANTISPAM: Programma o tecnologia che impedisce, o quantomeno limita, la ricezione di posta indesiderata nella propria casella di posta in entrata.

ANTISPYWARE: Il software antispyware protegge il computer da popup pubblicitari, lentezza e minacce alla sicurezza dovute a spyware e altro software indesiderato.

ANTIVIRUS: Programma che individua, previene e rimuove programmi dannosi, come virus e worm. Affinché sia efficace deve essere costantemente aggiornato.

ATTIVAZIONE: Procedura indispensabile, connessa all'installazione di molti software per attestare la genuinità.

BACKDOOR: Accesso abusivo a un sistema informatico. Di solito una backdoor viene inserita dagli stessi programmatori del sistema per poter effettuare accessi di emergenza, ma a volte gli hacker riescono a individuarle sfruttandole a proprio vantaggio.

BACKUP: Operazione che consiste nel salvare periodicamente i dati memorizzati sul disco fisso del PC. È indispensabile fare backup frequenti perché un virus, un guasto dell'hardware, un incendio o anche un'operazione sbagliata possono causare la perdita dei dati.

BOT: Il termine bot è un'abbreviazione di "robot". I pirati informatici li usano per trasformare il tuo computer in un dispositivo in grado di effettuare automaticamente operazioni su Internet a tua insaputa.

CHAT: Significa "chiacchierare" e indica le conversazioni scritte in tempo reale che si possono fare in rete con altri utenti tramite appositi programmi per esempio Messenger e Skype. Nelle versioni più evolute le Chat prevedono la possibilità di parlare sfruttando microfono e casse del PC o addirittura di effettuare video conversazioni.



CLOUD: Il termine inglese cloud computing indica un insieme di tecnologie che permettono di memorizzare ed elaborare dati grazie all'utilizzo di risorse hardware e software distribuite e virtualizzate in Rete. SkyDrive e le Office Web Apps sono un esempio di servizio cloud offerto gratuitamente da Microsoft.

CONTROLLO ACTIVE X: I controlli ActiveX sono piccoli programmi che vengono utilizzati su Internet. Nella maggior parte dei casi sono utili, per esempio per l'installazione di aggiornamenti di sicurezza, ma se usati illegalmente possono effettuare attività senza il tuo controllo.

COOKIE: I Cookie sono piccoli file che i siti web salvano sul tuo disco rigido alla tua prima visita. Il loro compito è quello di ricordare i tuoi dati quando ritorni a visitare un sito. Generalmente I cookie non sono dannosi, ma se usati in maniera fraudolenta possono sottrarre informazioni a tua insaputa.

COPYRIGHT: È il diritto d'autore che stabilisce la proprietà intellettuale di un'opera.¹⁷

CRACCARE: Neologismo gergale da "to crack", "spezzare". Si intende il superamento delle protezioni di un programma o di un sistema informatico.

CRACK: Un sistema generalmente software, in grado di eliminare le protezioni che vengono normalmente applicate ai programmi per evitare che vengano duplicati e installati illecitamente. L'utilizzo dei crack è illegale.

CRACKER: Declinazione negativa dell'hacker. Quest'ultimo generalmente viola i sistemi informatici solo per metterli alla prova, mentre il Cracker lo fa con l'obiettivo di sottrarre i dati, danneggiare i sistemi o sottrarre denaro, per esempio da un conto corrente on line.

CYBERBULLISMO: Termine che identifica attività di bullismo perpetrate tramite internet. Segnala l'episodio di bullismo al sito Web in cui è avvenuto. Molti servizi si avvalgono di moderatori e di luoghi in cui segnalare gli abusi, ad esempio abuseramicrosoft.com.



CYBERPEDOFILIA: Il pedofilo telematico è un individuo estremamente pericoloso perché spesso è difficile da individuare. Tipicamente cerca di instaurare un clima di fiducia e di amicizia fingendosi coetaneo dei bambini e cercando di agire quando il minore non è controllato da persone adulte.

DIALER: È uno speciale programma auto-eseguibile che altera i parametri della connessione a internet impostati sul computer dell'utente, agendo sul numero telefonico del collegamento e sostituendolo con un numero a pagamento maggiorato su prefissi internazionali satellitari o speciali.

DISCLAIMER: Significa "Esonero di responsabilità". L'insieme dei diritti e doveri dell'utente e limitazioni di responsabilità del produttore, relative a un software, da accettare al momento dell'installazione.

DRM: Acronimo di Digital Right Management, standard ideato da Microsoft sulla gestione dei diritti relativo alle opere digitali protette da copyright.

FAKE: Identifica un falso, Su Internet usato spesso per identificare l'utilizzo di un'identità falsa o altrui, un file fasullo o un allarme relativo a un virus inesistente.

FILE SHARING: Scambio di file solitamente attraverso reti paritarie [p2p], ma anche attraverso apposite piattaforme. Può essere illegale.

FILTRO SMART SCREEN: Il filtro SmartScreen è una funzionalità di Internet Explorer 9 e 8 che ti aiuta a evitare le minacce sotto forma di malware, phishing e le truffe online quando navighi su Internet a evitare le minacce di ingegneria sociale, sotto forma di malware e phishing, e le truffe online quando navighi sul web

FIREWALL: Un firewall è un programma software o un componente hardware che permette di respingere gli attacchi di hacker, virus o worm che cercano di raggiungere il computer attraverso internet,

FIRMA DIGITALE: Procedura che garantisce l'integrità e l'autenticità di un documento informatico, in analogia con la firma autografata.

FLAME: Il termine significa "fiammata" ed è tipico dei newsgroup. Identifica un attacco o reazione aggressiva verbale nei confronti di un utente.



FURTO DI IDENTITÀ: Il furto di identità è un qualsiasi tipo di frode che porta alla perdita di dati personali, come password, nomi utente, dati bancari o numeri di carte di credito. La forma più diffusa è il phishing, ovvero la frode perpetrata tramite mail

HACKER: Nella sua forma più pura si può considerare una sorta di studioso dei sistemi informati, che tenta di violare per saggiarne i limiti e la sicurezza senza provocare danni. Purtroppo sempre più spesso gli hacker diventano cracker, ovvero persone che lo fanno a scopo di lucro, per sottrarre dati o per mettere fuori uso i sistemi informatici.

HTTPS: l'utilizzo del protocollo HTTPS [Hyper text Transfer Protocol Secure] consente di proteggere le informazioni inviate in Internet. In Hotmail viene per esempio utilizzato il protocollo HTTPS per la crittografia delle informazioni di accesso.

ICRA: Internet Content Rating Association. Un'associazione internazionale senza fini di lucro nata per difendere e aiutare la navigazione dei minori in Rete.

INPRIVATE BROWSING: Tecnologia che consente di evitare che la cronologia delle esplorazioni, i file internet temporanei, i dati dei moduli, i cookie nonché i nomi utente e le password vengano mantenuti nel browser. In questo modo non lascerai traccia della tua navigazione

LOGIN: Procedura di accesso a un computer, a un programma o a un servizio, generalmente legata all'inserimento di un username e di una password. È fondamentale scegliere password sicure per evitare che altri possano accedere senza il nostro consenso,

LURKER: Chi sta in agguato. Nelle attività in rete indica chi osserva senza prendere parte attiva.

MALWARE: Malware è l'abbreviazione di "malicious software", ovvero software dannoso. Con questo termine si identifica un software che viene installato senza il tuo consenso, per esempio mentre scarichi un programma gratuito o un file da una rete peer to peer.

MICROSOFT SECURITY ESSENTIALS: Microsoft Security Essentials è un software antimalware gratuito per il tuo computer. Ti protegge da virus, spyware e altro malware. È scaricabile gratuitamente per Windows 7, Windows Vista e Windows XP SP2 e superiori.



NETIQUETTE: Contrazione di Net Etiquette, ovvero "etichetta di rete". Insieme di regole che disciplinano il comportamento di un utente in internet. Il rispetto della netiquette non è imposto da alcuna legge, ma è prassi comune attenersi.

NETIZEN: Il termine significa "cittadino della Rete". Neologismo abbastanza usato derivato da network e citizen.

NEWBIE: Neologismo gergale che indica un nuovo utente della rete, un navigatore alle prime armi.

HOAX (FINTE MAIL): Un fenomeno legato al phishing e al furto di identità. Si tratta di finte mail, per esempio provenienti da istituti bancari o altri organismi, il cui unico scopo è sottrarre informazioni personali.

NICKNAME: Quando non si vuole usare il proprio nome in rete, si può scegliere un soprannome, detto appunto nickname. Non è possibile sapere chi si nasconde dietro a un nickname, per questo occorre fare molta attenzione quando si naviga in rete e ci si raffronta con altri utenti.

PEER- TO-PEER: Architettura di rete nella quale tutti i computer funzionano sia come client sia come server. Tutti i computer sono quindi uguali e di pari livello. Un esempio di rete peer-to-peer è Emule. Spesso questo tipo di reti vengono utilizzate per scambiare file illegalmente.

PHARMING: Tecnica che permette di sfruttare a proprio vantaggio le vulnerabilità di server controllando il dominio di un sito e utilizzandolo per ridirigere il traffico su altro sito.

PARENTAL CONTROL: Un filtro che permette di bloccare la visione dei contenuti non adatti ai bambini o a persone particolarmente sensibili

PHISHING: Il phishing è un furto di identità on line. Si basa su e-mail, notifiche esiti web fraudolenti progettati per rubare dati personali o informazioni riservate come dati account, numeri di carte di credito, password o altro.

POP-UP: Il termine significa "saltar su" e indica le finestre che si aprono nel browser in modo automatico, di solito a scopi pubblicitari.



PROXY SERVER: Un server che si interpone tra i computer di chi naviga e il Web. Il suo scopo è sia quello di incrementare le prestazioni di navigazione, verificando se la pagina richiesta è già disponibile in memoria, sia di filtrare la navigazione, per esempio per impedire ai dipendenti di visitare siti vietati o aree particolari.

RIPPER: Letteralmente "squartatore". È così definito un programma che acquisisce i dati da CD musicale a DVD video e li importa sul disco fisso, per un'eventuale conversione e modifica. Questo genere di azioni è quasi sempre illegale.

SPAM: Lo spam è qualsiasi tipo di comunicazione on line indesiderata. Attualmente la forma più comune di spam è la posta elettronica, per questo sono nate tecnologie, come il filtro SmartScreen di Microsoft, che riduce drasticamente la posta indesiderata in grado di raggiungere la nostra casella di posta.

SPYWARE: Spyware è un termine che descrive un software che si installa sul computer senza il tuo consenso. Uno spyware può fare pubblicità, raccogliere informazioni personali e addirittura arrivare a modificare la configurazione del tuo computer.

SSL: Acronimo di "Secure Sockets layer", un protocollo che rende sicure le transazioni commerciali in rete, per esempio con carte di credito, grazie alla trasmissione dei dati cifrata.

TRACKING PROTECTION LIST: La TPL o Protezione da monitoraggio, permette di scegliere i siti autorizzati a ricevere le informazioni che riguardano la navigazione da parte dell'utente e di controllare la propria privacy durante la navigazione.

TROJAN: È un software che nasconde al suo interno un virus. Installando ed eseguendo il programma che contiene il Trojan, l'utente innesca il virus.

VIRUS: I virus informatici sono software progettati per diffondersi da un computer all'altro e interferire con il funzionamento della macchina. Un virus può cancellare dati, carpire informazioni, usare il programma di posta per diffondersi ad altre macchine e addirittura rendere il PC inutilizzabile.

Warez: Neologismo usato per individuare software scaricabili abusivamente e



illegalmente dalla rete.

WEP: Acronimo di Wired Equivalent Privacy, un sistema di crittografia che si basa su una chiave pubblica. Serve per rendere più sicure le comunicazioni wireless. Fa parte dei protocolli di sicurezza wireless anche l'algoritmo di crittografia AES, sigla di Advance Encryption Standard.

WORM: Un worm è un particolare virus informatico in grado di propagarsi senza la necessità che l'utente inneschi il suo funzionamento compiendo un'operazione, per esempio installando un software.

Sitografia:

<https://www.commissariatodips.it/>

<http://www.generazioniconnesse.it/site/it/home-page/>