Cittadinanza Digitale Consapevole

Diritti, Doveri e Uso Responsabile del Web

Classe II Indirizzo Informatica

Educazione Civica

A.S. 2024/2025

1. Che cosa è la Cittadinanza Digitale?

La cittadinanza digitale rappresenta l'insieme di competenze, conoscenze e comportamenti necessari per partecipare attivamente e responsabilmente alla comunità digitale moderna.

I Tre Pilastri Fondamentali

- **Accesso consapevole**: Capacità di trovare, valutare e utilizzare informazioni online in modo critico e sicuro
- **Uso responsabile**: Comportamenti etici nella creazione e condivisione di contenuti digitali
- **Protezione**: Salvaguardia dell'identità digitale, della privacy personale e della sicurezza informatica

Nel 2024, oltre l'85% della popolazione italiana è connessa a Internet: essere cittadini digitali consapevoli è ormai indispensabile.

2. Il Quadro Normativo di Riferimento

Il framework legislativo che regola la cittadinanza digitale si basa su norme europee e nazionali:

- **DigComp 2.2 (2022)**: Framework europeo delle competenze digitali per i cittadini, che identifica 21 competenze organizzate in 5 aree (informazione, comunicazione, creazione contenuti, sicurezza, problem solving)
- **Linee Guida MIUR 2023**: Integrazione dell'educazione civica digitale come insegnamento trasversale obbligatorio per almeno 33 ore annue in tutti gli ordini di scuola
- **GDPR (Regolamento UE 2016/679)**: Protezione dei dati personali a livello europeo, garantisce il controllo sui propri dati e stabilisce obblighi per chi li tratta
- **Legge 71/2017**: Disposizioni a tutela dei minori per la prevenzione e il contrasto del cyberbullismo

3. I Diritti del Cittadino Digitale

Ogni cittadino digitale gode di diritti fondamentali che vanno conosciuti e tutelati:

- **Diritto all'Accesso**: Garantire a tutti la possibilità di connettersi alla rete, abbattendo il digital divide geografico, economico e culturale. In Italia ancora il 15% della popolazione non ha accesso regolare a Internet
- **Diritto alla Privacy**: Controllare i propri dati personali, sapere chi li raccoglie, per quali finalità e poter chiederne la cancellazione (diritto all'oblio). Include la protezione da profilazione invasiva
- **Diritto alla Libertà di Espressione**: Manifestare liberamente il proprio pensiero online senza censure preventive, nel rispetto della dignità altrui e dei limiti previsti dalla legge (no diffamazione, incitamento all'odio)
- **Diritto all'Identità Digitale**: Costruire e gestire la propria presenza online in modo autentico e sicuro

4. I Doveri del Cittadino Digitale

Ai diritti corrispondono precise responsabilità verso la comunità digitale:

Responsabilità Legali e Sociali

- **Rispettare la legge**: Le norme del mondo reale valgono anche online (no diffamazione, minacce, violazione copyright, stalking digitale). La pena per diffamazione online è aggravata
- **Verificare le fonti**: Prima di condividere una notizia, controllarne l'attendibilità attraverso il fact-checking. Il 67% delle fake news viene diffuso per superficialità, non per malafede
- **Proteggere l'ambiente digitale**: Utilizzare password sicure, aggiornare i software, non diffondere malware, segnalare contenuti illeciti, rispettare la netiquette
- **Essere rispettosi**: Evitare linguaggio offensivo, flame war e comportamenti che possano danneggiare la dignità altrui

5. Identità Digitale in Italia: SPID e CIE

L'identità digitale è il sistema che permette di accedere ai servizi online con credenziali certificate:

SPID (Sistema Pubblico Identità Digitale)

- Credenziali uniche per tutti i servizi della PA
- 3 livelli di sicurezza crescente
- Oltre 35 milioni di identità attive
- Riconosciuto anche da privati

CIE e Strumenti Associati

- Carta Identità Elettronica con chip NFC
- Funzione di accesso ai servizi online
- PEC: Posta certificata con valore legale
- Domicilio digitale per notifiche PA

Dal 2025 l'IT Wallet integrerà documenti digitali, pagamenti e servizi in un'unica app.

6. Email: Strumento Fondamentale di Comunicazione

L'email rimane lo strumento professionale più utilizzato per la comunicazione formale:

- **Traccia permanente**: Ogni email lascia una documentazione scritta consultabile nel tempo, utile per conferme e verifiche
- **Valore probatorio**: In molti contesti legali e professionali l'email ha valore di prova documentale
- **Porta d'accesso professionale**: Primo contatto con università, datori di lavoro, istituzioni. La qualità della comunicazione via email riflette la professionalità
- **Differenza da chat**: A differenza dei messaggi istantanei, l'email richiede maggiore formalità, struttura e riflessione prima dell'invio

Nel mondo professionale si stima che un dipendente riceva in media 120 email al giorno: saper comunicare efficacemente è essenziale.

7. Netiquette della Posta Elettronica

La netiquette è l'insieme delle regole di buon comportamento nella comunicazione digitale:

1. **Oggetto chiaro e specifico**: Deve riassumere il contenuto in 5-8 parole. Es. "Richiesta informazioni progetto DigComp" invece di "Domanda"
2. **Saluti appropriati**:
   - Formale: "Gentile Prof./Dott.", "Cordiali saluti"
   - Informale tra pari: "Ciao [Nome]", "A presto"
3. **Corpo del messaggio**: Breve (max 200 parole), strutturato in paragrafi, con richiesta esplicita se necessario
4. **Firma**: Nome completo, ruolo/classe, contatti (se professionale)
5. **Risposta tempestiva**: Idealmente entro 24-48 ore lavorative
6. **Tono professionale**: Evitare abbreviazioni da chat, emoji eccessive, tono aggressivo

8. Errori Comuni da Evitare nella Email

Questi errori possono compromettere la comunicazione e la reputazione professionale:

Errore	**Effetto e Soluzione**
Tutto in MAIUSCOLO	Equivale a urlare. Usare normale capitalizzazione
Allegati troppo grandi	Blocco casella (max 10-25 MB). Usare servizi cloud con link
Oggetto vuoto o generico	Email ignorata o finisce in spam. Essere specifici
Rispondere a tutti inutilmente	Sovraccarico caselle. Usare "Rispondi" selettivamente
Errori grammaticali	Impressione di superficialità. Rileggere prima di inviare
Inviare senza controllare	Destinatari sbagliati o allegati mancanti

9. Protezione della Privacy nella Posta Elettronica

L'email è uno dei principali vettori di attacco informatico e violazione della privacy:

- **Uso del BCC/CCN (Copia Carbone Nascosta)**: Quando si invia a gruppi, usare CCN per non esporre gli indirizzi di tutti i destinatari. Protezione GDPR
- **Anti-Phishing**:
  - Non cliccare su link sospetti o allegati inattesi
  - Verificare il mittente (attenzione a domini simili: paypa1.com vs paypal.com)
  - Nessuna banca/istituzione seria chiede password via email
- **Autenticazione a Due Fattori (2FA)**: Attivare sempre la verifica in due passaggi (password + codice SMS/app). Riduce del 99,9% i rischi di accesso non autorizzato
- **Password robuste**: Almeno 12 caratteri, combinazione maiuscole/minuscole/numeri/simboli, diverse per ogni account
- **Aggiornamenti**: Mantenere aggiornato il client email per patch di sicurezza

10. Email Istituzionale: Responsabilità e Buone Pratiche

L'account scolastico (@istituto.edu.it) è uno strumento professionale che richiede uso appropriato:

- **Solo uso didattico**: Non per registrazioni a social media, gaming, shopping online. Uso monitorato dall'istituto per finalità educative
- **Linguaggio formale con docenti**:
  - Usare "Gentile Prof./Prof.ssa" non "Ciao"
  - Specificare classe e sezione
  - Firmare con nome e cognome
- **Sicurezza**:
  - Non condividere la password con compagni
  - Non iscriversi a siti non verificati
  - Segnalare email sospette ai docenti
- **Conservazione**: Controllare regolarmente la casella, archiviare comunicazioni importanti
- **Conseguenze uso improprio**: L'account può essere sospeso e l'uso inappropriato può avere implicazioni disciplinari

11. Navigazione Web Consapevole: Pensiero Critico

Navigare consapevolmente significa sviluppare capacità di analisi e valutazione delle fonti online:

- **Valutare l'autorevolezza**:
  - Chi ha scritto il contenuto? Verificare credenziali e competenze
  - Il sito è riconosciuto (università, enti di ricerca, testate giornalistiche registrate)?
  - Presenza di riferimenti bibliografici e fonti citabili?
- **Distinguere contenuti**:
  - Fatti vs opinioni personali
  - Articoli informativi vs contenuti sponsorizzati (native advertising)
  - Ricerche scientifiche vs blog personali
- **Cross-checking**: Verificare la stessa informazione su almeno 2-3 fonti indipendenti e autorevoli prima di considerarla attendibile
- **Data di pubblicazione**: Le informazioni sono aggiornate? Particolarmente importante per tecnologia, medicina, attualità

12. Come Riconoscere le Fake News

Le notizie false si diffondono 6 volte più velocemente di quelle vere. Ecco come individuarle:

Segnali di Allarme (Red Flags)

- **Titoli sensazionalistici**: "SHOCK!", "Non crederai mai", "Stanno nascondendo la verità". Mirano a suscitare emozioni forti per ottenere click
- **URL sospetti**: Domini storpiati (amzon.co invece di amazon.com), suffissi insoliti (.co.de, .news-24)
- **Assenza di firma**: Articoli senza autore identificabile o data di pubblicazione
- **Immagini fuori contesto**: Foto di eventi diversi spacciati per attuali. Usare Google Images per verificare l'origine
- **Errori grammaticali**: Testi mal scritti, pieni di refusi
- **Assenza di altre fonti**: Se solo un sito riporta la notizia "bomba", probabilmente è falsa

Strumenti utili: Factcheckers italiani (Pagella Politica, Open, Butac), Google News Lab

13. Parametri di Sicurezza nella Navigazione Web

Identificare siti sicuri e affidabili protegge da furti di dati e truffe:

- **HTTPS (HyperText Transfer Protocol Secure)**:
  - Protocollo che cripta i dati tra browser e server
  - Essenziale per e-commerce, banking, inserimento password
  - Visibile nell'URL: https:// invece di http://
- **Certificato SSL/TLS valido**:
  - Simbolo del lucchetto chiuso nella barra indirizzi
  - Cliccandolo si vedono i dettagli del certificato
  - Attenzione: il lucchetto indica solo la crittografia, non l'affidabilità del sito
- **Informazioni legali trasparenti**:
  - Presenza nel footer: P.IVA, ragione sociale, contatti
  - Privacy policy e cookie policy chiare
  - Per e-commerce: reso, garanzie, modalità di pagamento
- **Recensioni e reputazione**: Verificare su Trustpilot o forum specializzati

14. Introduzione ai Social Media: Opportunità e Rischi

I social media sono ambienti complessi di relazione, informazione e costruzione dell'identità:

- **Diffusione in Italia**:
  - 67% degli adolescenti (13-19 anni) connessi quotidianamente
  - Età media primo smartphone: 11 anni
  - Piattaforme più usate: Instagram, TikTok, YouTube, Snapchat
- **Cambio di paradigma**:
  - Da consumatori passivi a produttori attivi di contenuti
  - Responsabilità su ciò che si pubblica e si condivide
  - Permanenza digitale: "ciò che pubblichi resta"
- **Funzioni principali**:
  - Socializzazione e mantenimento relazioni
  - Informazione e intrattenimento
  - Espressione creativa e costruzione identità
  - Marketing e influencer economy

L'uso consapevole richiede equilibrio tra opportunità sociali e protezione del benessere personale.

15. Diritti e Doveri sui Social Media

Anche sui social valgono regole chiare per una convivenza digitale rispettosa:

I Tuoi Diritti

- Essere protetto da insulti, molestie e cyberbullismo
- Controllare chi vede i tuoi contenuti
- Segnalare contenuti inappropriati
- Richiedere la cancellazione dei tuoi dati
- Non subire discriminazioni

I Tuoi Doveri

- Non diffondere foto/video altrui senza consenso (violazione privacy)
- Non insultare o deridere altri utenti
- Verificare notizie prima di condividerle
- Rispettare il copyright su immagini e musica
- Non impersonare altre persone

Ricorda

Pubblicare foto di minori senza autorizzazione dei genitori è reato. Anche condividere una foto ricevuta in privato può costituire violazione della privacy.

16. La Tua Impronta Digitale: Gestire la Reputazione Online

Ogni attività online lascia tracce permanenti che costruiscono la tua identità digitale:

- **"Internet non dimentica"**:
  - Screenshot, cache, archivi web conservano contenuti anche dopo la cancellazione
  - Post impulsivi fatti a 14 anni possono riemergere anni dopo
  - La reputazione digitale si costruisce nel tempo e si distrugge in un attimo
- **Social screening professionale**:
  - Il 70% dei datori di lavoro verifica i profili social dei candidati
  - Università e istituzioni controllano l'impronta digitale nelle selezioni
  - Contenuti inappropriati possono precludere opportunità professionali
- **Coerenza identitaria**:
  - Mantenere coerenza tra vita reale e profilo digitale
  - Evitare contraddizioni tra diversi profili social
  - Curare l'immagine professionale (LinkedIn) separandola da quella personale

Consiglio: Googla periodicamente il tuo nome per verificare cosa emerge sulla tua persona.

17. Proteggere la Privacy sui Social Media

Configurare correttamente le impostazioni di privacy è fondamentale per la sicurezza online:

- **Profilo privato**:
  - Rendere l'account visibile solo agli amici approvati
  - Su Instagram/TikTok: attivare "Account privato"
  - Valutare attentamente le richieste di amicizia
- **Gestione dei tag**:
  - Attivare l'approvazione manuale prima che una foto taggata appaia sul profilo
  - Rimuovere tag indesiderati da foto altrui
  - Limitare chi può taggarti
- **Visibilità dei contenuti**:
  - Impostare la visibilità predefinita su "Solo amici" anziché "Pubblico"
  - Usare le liste personalizzate per condividere con gruppi specifici
  - Disattivare la geolocalizzazione automatica dei post
- **Informazioni personali**: Nascondere numero di telefono, email, data di nascita completa, indirizzo di casa

18. Cyberbullismo: Riconoscerlo e Contrastarlo

Il cyberbullismo è una piaga sociale con conseguenze psicologiche gravi sulle vittime:

Definizione (Legge 71/2017)

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 online 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 distintive:

- **Intenzionalità**: Atto deliberato di fare del male
- **Ripetizione**: Comportamento sistematico nel tempo
- **Squilibrio di potere**: Vittima in difficoltà a difendersi
- **Amplificazione**: Il contenuto può diventare virale rapidamente

19. Strategie di Contrasto al Cyberbullismo

Azioni concrete per vittime, testimoni e comunità educativa:

Se sei vittima:

- **Non rispondere**: Evitare escalation
- **Bloccare**: Impedire ulteriori contatti
- **Documentare**: Screenshot come prove
- **Parlare**: Confidarsi con adulti fidati (genitori, docenti, psicologo)
- **Segnalare**: Utilizzare strumenti di segnalazione delle piattaforme

Se sei testimone:

- **Non ridere**: Non alimentare il bullo
- **Non condividere**: Bloccare la diffusione
- **Supportare**: Messaggio privato alla vittima
- **Segnalare**: Al referente cyberbullismo della scuola
- **Denunciare**: Casi gravi alla Polizia Postale

Referente Cyberbullismo

Ogni scuola ha un docente referente. In caso di necessità, rivolgersi a questa figura o al coordinatore di classe.

20. Dipendenza Digitale e Benessere Psicologico

L'uso eccessivo di dispositivi digitali può generare dipendenza e problemi di salute:

- **Nomofobia**: Paura di rimanere senza smartphone. Il 53% degli adolescenti prova ansia se non può controllare il telefono
- **FOMO (Fear Of Missing Out)**:
  - Paura di perdersi eventi/esperienze sociali
  - Controllo compulsivo dei social per rimanere aggiornati
  - Ansia da esclusione sociale
- **Impatti sulla salute fisica**:
  - Disturbi del sonno (luce blu, notifiche notturne)
  - Problemi posturali e affaticamento visivo
  - Sedentarietà eccessiva
- **Impatti psicologici**:
  - Confronto sociale costante: "Gli altri hanno vite migliori"
  - Calo dell'autostima e depressione
  - Riduzione capacità di concentrazione e attenzione
  - Isolamento sociale paradossale (connessi ma soli)

21. Strategie per un Uso Equilibrato della Tecnologia

Il benessere digitale richiede consapevolezza e autodisciplina:

- **Monitoraggio del tempo**:
  - Utilizzare app integrate (Screen Time iOS, Benessere Digitale Android)
  - Impostare limiti giornalieri per app specifiche (es. max 1h social)
  - Analizzare statistiche settimanali di utilizzo
- **Zone e momenti "No-Phone"**:
  - Durante i pasti in famiglia (favorisce dialogo)
  - Un'ora prima di dormire (migliora qualità del sonno)
  - Durante lo studio concentrato (tecnica Pomodoro)
  - In presenza di amici (presenza autentica)
- **Attività alternative offline**:
  - Sport, hobby creativi (disegno, musica, scrittura)
  - Lettura di libri cartacei
  - Attività all'aperto e socializzazione diretta
- **Notifiche intelligenti**: Disattivare notifiche non essenziali, attivare modalità "Non disturbare"

22. Algoritmi, Echo Chambers e Disinformazione

I social media utilizzano algoritmi che influenzano significativamente ciò che vediamo:

- **Come funzionano gli algoritmi**:
  - Analizzano comportamento (like, condivisioni, tempo di visualizzazione)
  - Mostrano contenuti simili a quelli già apprezzati
  - Obiettivo: massimizzare engagement (tempo sulla piattaforma)
- **Echo Chambers (Camere dell'eco)**:
  - Vediamo solo contenuti che confermano le nostre opinioni
  - Rafforzamento dei pregiudizi esistenti
  - Difficoltà nel confronto con posizioni diverse
  - Polarizzazione sociale crescente
- **Amplificazione fake news**:
  - Le notizie false generano più emozioni (rabbia, paura)
  - Contenuti emotivi = più engagement = maggiore diffusione algoritmica
  - Studi dimostrano: fake news si diffondono 6 volte più velocemente delle notizie vere

Soluzione: Diversificare le fonti, seguire account con opinioni diverse, fact-checking sistematico

23. Diritto all'Oblio nel GDPR

Il diritto alla cancellazione dei dati personali è un principio fondamentale del GDPR:

Definizione (Art. 17 GDPR): L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo.

Quando si può esercitare:

- I dati **non sono più necessari** rispetto alle finalità per cui erano stati raccolti
- L'interessato **revoca il consenso** e non esiste altra base giuridica per il trattamento
- I dati sono stati **trattati illecitamente** (raccolti senza autorizzazione)
- L'interessato **si oppone al trattamento** e non sussistono motivi legittimi prevalenti
- La cancellazione è **necessaria per obbligo legale**

Limiti: Il diritto non si applica quando è necessario per:

- Esercizio del diritto alla libertà di espressione e informazione
- Adempimento di obblighi legali
- Motivi di interesse pubblico (sanità, ricerca scientifica)

24. Le Competenze Digitali del Futuro: DigComp 2.2

Il framework europeo identifica 21 competenze digitali organizzate in 5 aree:

1. **Alfabetizzazione su informazioni e dati**:
   - Navigare, ricercare e filtrare dati e contenuti digitali
   - Valutare dati, informazioni e contenuti digitali
   - Gestire dati, informazioni e contenuti digitali
2. **Comunicazione e collaborazione**:
   - Interagire attraverso le tecnologie digitali
   - Condividere informazioni attraverso le tecnologie digitali
   - Collaborare attraverso le tecnologie digitali
   - Gestire l'identità digitale
3. **Creazione di contenuti digitali**:
   - Sviluppare contenuti digitali (come questa presentazione!)
   - Integrare e rielaborare contenuti digitali
   - Rispettare copyright e licenze

24. DigComp 2.2 (continua)

4. **Sicurezza**:
   - Proteggere i dispositivi
   - Proteggere i dati personali e la privacy
   - Proteggere la salute e il benessere
   - Proteggere l'ambiente
5. **Risolvere problemi**:
   - Risolvere problemi tecnici
   - Identificare i bisogni e le risposte tecnologiche
   - Utilizzare in modo creativo le tecnologie digitali
   - Identificare i divari di competenze digitali

Ogni competenza è articolata su 8 livelli di padronanza, da Base a Altamente specializzato. L'obiettivo UE è che l'80% dei cittadini raggiunga almeno competenze digitali di base entro il 2030.

25. Bilancio Critico dei Social Media

Un'analisi equilibrata degli impatti psicologici e sociali dei social media:

Aspetti Positivi

- Connessione con persone lontane geograficamente
- Supporto sociale in comunità online (gruppi di interesse, supporto psicologico)
- Accesso democratizzato all'informazione
- Opportunità creative ed espressive
- Mobilitazione sociale e attivismo
- Opportunità professionali e networking

Criticità e Rischi

- Cyber-esclusione e cyberbullismo
- Distrazione cognitiva e frammentazione dell'attenzione
- Dipendenza comportamentale
- Confronto sociale dannoso
- Diffusione disinformazione
- Violazione della privacy
- Filter bubbles e polarizzazione

Conclusione

I social media sono strumenti neutri: l'impatto dipende dalle modalità d'uso. L'educazione alla cittadinanza digitale è essenziale per massimizzare i benefici e minimizzare i rischi.

26. Sintesi: Protezione Digitale a 360 Gradi

Un approccio integrato alla sicurezza informatica personale:

- **Gestione Password**:
  - Password diverse e complesse per ogni servizio (min 12 caratteri)
  - Uso di password manager (Bitwarden, 1Password, KeePass)
  - Cambio periodico delle password critiche (banking, email principale)
  - Mai salvare password in file non criptati
- **Sicurezza Navigazione**:
  - Browser aggiornato all'ultima versione
  - Antivirus/antimalware attivo e aggiornato
  - Evitare reti WiFi pubbliche per operazioni sensibili (o usare VPN)
  - Cancellare periodicamente cookie e cronologia
- **Privacy sui Social**:
  - Geolocalizzazione disattivata di default
  - Revisione periodica delle impostazioni privacy (cambiano spesso!)
  - Limitare app di terze parti collegate ai social

27. Responsabilità Giuridica nel Mondo Digitale

Il diritto penale e civile si applicano pienamente anche alle condotte online:

Principio fondamentale: Non esiste "immunità digitale". Le leggi del mondo fisico valgono anche online.

Reati più comuni:

- **Diffamazione aggravata** (Art. 595 c.p.): Offendere la reputazione di qualcuno online. Aggravante: mezzo di pubblicità (social = diffusione potenzialmente virale). Pena: reclusione fino a 3 anni
- **Stalking telematico** (Art. 612-bis c.p.): Molestie reiterate che causano ansia o timore. Include messaggi ossessivi, controllo GPS, revenge porn
- **Violazione copyright** (Legge 633/1941): Distribuzione non autorizzata di opere protette (film, musica, software, immagini). Sanzioni civili e penali
- **Accesso abusivo a sistema informatico** (Art. 615-ter c.p.): Entrare in account altrui (anche se la password era facile da indovinare)
- **Sostituzione di persona** (Art. 494 c.p.): Creare profili fake spacciandosi per altri

Anche i minorenni possono essere imputabili penalmente dai 14 anni. I genitori rispondono civilmente dei danni causati dai figli.

28. Risorse e Contatti Utili per Supporto

Servizi istituzionali e organizzazioni di supporto per situazioni problematiche:

- **Generazioni Connesse** (`generazioniconnesse.it`):
  - Portale del MIUR per uso sicuro di internet
  - Materiali didattici per scuole e famiglie
  - Helpline 1.96.96 per segnalazioni
- **Polizia Postale** (`commissariatodips.it`):
  - Segnalazione reati informatici
  - Sportelli in ogni provincia italiana
  - Form online per denunce
- **Telefono Azzurro** (19696):
  - Supporto psicologico h24 per minori
  - Consulenza su cyberbullismo e abusi online
  - Chat disponibile sul sito `azzurro.it`
- **Garante Privacy** (`garanteprivacy.it`): Reclami per violazioni GDPR
- **AGCOM** (`agcom.it`): Segnalazione contenuti illegali online

29. Il Tuo Impegno come Cittadino Digitale

La cittadinanza digitale è una responsabilità attiva, non una condizione passiva:

Manifesto del Cittadino Digitale Consapevole

"Sii il cambiamento che vuoi vedere nel web"

1. **Rispetta la privacy**: Tua e altrui. Pensa prima di pubblicare foto di altre persone
2. **Verifica prima di condividere**: Non essere complice della disinformazione. Fact-checking sempre
3. **Proteggi la tua identità**: Password sicure, 2FA attiva, informazioni personali limitate
4. **Sii gentile**: Il linguaggio online ha conseguenze reali. Tratta gli altri con rispetto
5. **Pensa al lungo termine**: La tua reputazione digitale ti seguirà per anni
6. **Chiedi aiuto**: In caso di problemi, rivolgersi ad adulti fidati e autorità competenti

La tecnologia è un moltiplicatore: amplifica sia il bene che il male. La scelta di come utilizzarla è nelle tue mani.

30. Glossario dei Termini Tecnici

- **Phishing**: Tecnica di truffa informatica per rubare credenziali fingendosi enti affidabili via email/SMS
- **Netiquette**: Insieme di regole di comportamento e buone maniere nella comunicazione digitale (network + etiquette)
- **Malware**: Software dannoso progettato per danneggiare sistemi o rubare dati (virus, trojan, ransomware, spyware)
- **Cloud**: Servizio di archiviazione e elaborazione dati su server remoti accessibili via internet
- **2FA/MFA**: Autenticazione a due/più fattori. Sistema di sicurezza che richiede due prove di identità
- **SSL/TLS**: Protocolli di crittografia che garantiscono comunicazioni sicure su internet (HTTPS)
- **Cookie**: File di testo salvati dal browser per memorizzare preferenze e tracciare attività
- **VPN**: Virtual Private Network. Connessione criptata per navigazione anonima e sicura
- **Firewall**: Sistema di protezione che filtra il traffico di rete in entrata/uscita
- **Ransomware**: Malware che cripta i file e chiede riscatto per il ripristino
- **Bot**: Programma automatico che esegue operazioni ripetitive (es. chatbot, social bot)
- **Deepfake**: Contenuto multimediale manipolato con AI per sostituire volti/voci in modo realistico