GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Progetto didattico
per le Scuole Secondarie di Secondo grado

Diventa ambasciatore della privacy

EDUCAZIONE DIGITALE

Per sensibilizzare le nuove generazioni sul tema della privacy e della protezione dei dati personali

Iniziativa finanziata dal Ministero delle Imprese e del Made in Italy - fondo a vantaggio dei consumatori.

Indice

1.

Condividere online con consapevolezza

L'iniziativa

Diventa Ambasciatore della Privacy è un'iniziativa realizzata dal **Garante per la protezione dei dati personali** con il supporto tecnico di **Skuola.net**, con l'obiettivo di sensibilizzare ed educare le nuove generazioni sul tema della privacy e della tutela dei dati personali.

Contenuti didattici per 10 ore formative di Educazione Civica

Grazie al **vostro prezioso supporto** e all'**adesione all'iniziativa da parte della vostra Scuola**, gli **studenti** avranno modo di **acquisire una maggiore conoscenza e consapevolezza dei rischi legati all'uso delle nuove tecnologie, del valore della privacy, del rispetto di sé stessi e degli altri** e, a conclusione del percorso didattico, potranno mettere in pratica quanto appreso attraverso la produzione di un **video di sensibilizzazione sulle tematiche affrontate in classe**.
Il **Kit Didattico** sarà un valido **strumento di supporto** per i docenti durante le **ore di Educazione Civica**, in particolare nel trattare quelle **tematiche fondamentali** che rientrano a pieno titolo nell'ambito dell'**Educazione alla Cittadinanza Digitale**, cui obiettivo è appunto quello di sviluppare la capacità degli studenti di avvalersi consapevolmente e responsabilmente degli strumenti tecnologici.
All'interno del kit, i ragazzi avranno a disposizione anche delle **Linee guida** con tutte le indicazioni necessarie per la **realizzazione del video richiesto per partecipare al Contest creativo**.

Privacy in un mondo iperconnesso

Dall'avvento della rivoluzione digitale, molti dei problemi identificati come centrali per la società negli ultimi cento anni, sono stati radicalmente ridefiniti.
Uno tra questi è sicuramente la questione riguardante la **privacy**.
Il suo profondo legame con i mutamenti tecnologici ha dischiuso orizzonti totalmente nuovi e complessi all'interno di un mondo iperconnesso.

La sfida posta dalla realtà contemporanea è quindi molto complicata: occorre operare un **bilanciamento tra le potenzialità dell'utilizzo delle nuove tecnologie e i rischi che tale utilizzo rappresenta per la privacy e i dati personali**.

I ragazzi sentono il bisogno naturale di relazionarsi, comunicare e condividere. La rete e i social network rispondono in maniera facile e immediata a questa esigenza, amplificando però le insidie di un uso improprio o addirittura fraudolento dei dati personali.
La scarsa consapevolezza del potere della Rete, soprattutto mentre si utilizzano Internet e i servizi ai quali la Rete consente di accedere è un problema importante. Le nuove generazioni spesso non sono sufficientemente informate sull'uso delle nuove tecnologie e si trovano di conseguenza esposte a possibili danni o, nei casi peggiori, a veri e propri abusi (furti d'identità, cyberbullismo, revenge porn).

Esiste quindi la possibilità di far convivere le opportunità offerte dalla Rete, con l'esigenza legittima di tutela della nostra privacy?
Certamente! **Conoscere e comprendere i concetti, i diritti e i rischi che ruotano intorno alla privacy e alla protezione dei dati personali è un passo fondamentale per tutelarci ed essere in grado di rispettare gli altri.**
Il ruolo della Scuola nell'affrontare queste tematiche, soprattutto dopo l'accelerazione del processo di digitalizzazione della didattica in seguito all'emergenza del Covid-19, è fondamentale per la formazione e l'accrescimento delle competenze dei **futuri cittadini digitali**.

Buona lezione!

II.

La privacy è rispetto, la privacy è un diritto

Cosa si intende per privacy e per valore del rispetto

Privacy è il termine con cui viene individuato quell'insieme di diritti e libertà connesse alla tutela della sfera privata e alla protezione dei dati personali dell'individuo.

Quando scarichiamo una nuova app, riflettiamo sul fatto che può avere accesso a molti dei dati contenuti nel nostro cellulare o nel nostro tablet?
Quando pubblichiamo contenuti sui social, pensiamo a quante persone sconosciute possono conoscere le nostre informazioni personali o le nostre foto e i nostri video?

Internet, gli smartphone, le app, i social sono delle memorie inesauribili di tutte le informazioni e i ricordi che condividiamo online, spesso con leggerezza.

Carta dei diritti fondamentali dell'Unione Europea

La Carta dei diritti fondamentali dell'Unione Europea sancisce che il diritto alla privacy rientra nella tutela della dignità umana.
In particolare:
Articolo 7
Rispetto della vita privata e della vita familiare
Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni
Articolo 8
Protezione dei dati di carattere personale
1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.
2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.
3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

La **privacy** ha ormai un ruolo centrale nelle nostre vite, eppure **ci preoccupiamo troppo poco di proteggerla**. In particolare i ragazzi che, pensando di doversi tutelare solo dal controllo genitoriale e scolastico, fanno sempre più fatica a tracciare una linea di confine tra pubblico e privato, a decidere consapevolmente cosa condividere con il mondo attraverso i social network.
A ogni età è importante essere consapevoli che **la tutela della sfera privata è un diritto fondamentale**.
I primi a rispettare la nostra privacy dobbiamo essere noi stessi.
Ma è importante ricordare che anche gli altri hanno diritto alla propria privacy, dobbiamo quindi valutare sempre le possibili conseguenze negative delle nostre azioni sul prossimo.

Quando parliamo di privacy parliamo dunque di rispetto: della persona, della dignità, dell'identità e della riservatezza di ognuno di noi.

È importante rispettare e far rispettare le regole che sono alla base della tutela dei nostri dati e la nostra riservatezza, ma soprattutto è importante contribuire a far crescere un'autentica cultura del rispetto. Questo rispetto è governato da norme, che per quanto riguarda la privacy, sono contenute nel GDPR, il Regolamento europeo sulla protezione dati.

Come siamo arrivati al GDPR?

Le origini moderne della privacy tradizionalmente si fanno risalire a due giuristi statunitensi, Samuel Warren e Louis Brandeis, che diedero alle stampe un saggio intitolato **The Right to Privacy. (1890)**[1], nato dall'esigenza di tutelarsi dagli eccessi della stampa che iniziava a focalizzarsi sempre di più sulla vita privata dei cittadini, noti e meno noti.
In Europa si ha una prima formazione del concetto di privacy tra fine '700 e gli inizi dell'800, ma la spinta a considerare riservatezza e protezione dei dati personali come diritti fondamentali specificamente espressi e costituzionalmente garantiti è venuta man mano crescendo nella seconda metà del secolo scorso.
Con la società sempre in continuo cambiamento e il diffuso utilizzo delle nuove tecnologie, è diventato sempre più **urgente il bisogno di tutelare le nostre informazioni personali dall'uso che potrebbero farne le altre persone.**

#DataPrivacyDay

Il **28 gennaio** è la giornata internazionale sulla sensibilizzazione e la promozione dell'importanza della privacy e della protezione dei dati.

È negli anni '90 che si arriva a un importante svolta con la **Direttiva 95/46 CE** [2], detta **Direttiva Madre**, che ha portato all'introduzione negli Stati membri dell'Unione Europea di una normativa organica sul trattamento dei dati personali con l'obiettivo di promuovere uno scambio di informazioni rispettoso dei diritti e delle libertà fondamentali di ogni cittadino europeo. Per preservare questo diritto in Italia, con la legge 675/96 sulla "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" viene istituita una autorità, il **Garante per la protezione dei dati personali**, con compiti di vigilanza e di controllo e con il potere di emanare provvedimenti e Linee guida. Nel **2003**, viene emanato il **d.lsg. 196/2003** [3], denominato "**Codice in materia di protezione dei dati personali**", che riordina e armonizza le disposizioni sulla tutela dei diritti della persona. Nel **2016** viene adottato il **Regolamento generale sulla protezione dei dati (UE) 2016/679 (GPDR)** [4] che sostituisce la vecchia direttiva dell'Unione Europea. Il Regolamento, entrato in vigore il 24 maggio 2016 e divenuto totalmente applicabile il 25 maggio 2018, introduce tutele e limiti che riguardano i minorenni. È importante, infatti, sapere che il GDPR stabilisce l'età necessaria per fornire il consenso al trattamento dei dati personali (16 anni), dando a ogni Stato la possibilità di stabilire un limite d'età diverso, che comunque non deve essere inferiore ai 13 anni. Nel nostro Paese l'età per poter esprimere il proprio consenso da parte dei minorenni è stabilita a 14 anni. Il trattamento dei dati personali del minore di età inferiore a 14 anni è lecito, a condizione che il consenso sia prestato o autorizzato da chi esercita la responsabilità genitoriale. Il GDPR e il Codice in materia di protezione dei dati personali costituiscono la normativa di riferimento in Italia.

Regolamenti

I REGOLAMENTI sono immediatamente vincolanti in tutto il territorio dell'UE, senza atti di recepimento, in modo uniforme (quindi è come se fossero delle leggi emanate dal Parlamento, solo che valgono per tutti i paesi dell'Unione).

Direttive

Le DIRETTIVE sono vincolanti per gli Stati nei fini, ma non nei mezzi; quindi fissano l'obiettivo, ma lasciano ai singoli Paesi uno spazio di interpretazione molto ampio e la possibilità di adottare norme nazionali che recepiscono le indicazioni della direttiva.

Suggerimento di attività didattica di cooperative learning:

Al termine della lezione, chiedete ai ragazzi di esprimere qual è per loro la differenza tra ciò che è personale e ciò che è pubblico e di confrontarsi per trovare insieme forme di comportamento utili a garantire la propria privacy rispettando comunque quella degli altri.

Link per approfondire:

1. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1768870
2. https://www.garanteprivacy.it/documents/10160/10704/Direttiva+95+46+CE.pdf/98ae1df8-185b-48cd-a107-ed8da71e05fe?version=1.3
3. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9042678
4. https://www.garanteprivacy.it/normativa-e-provvedimenti/gdpr-e-normativa-europea-e-internazionale

III.

Un post è per sempre

Per dato personale si intende "*qualsiasi informazione riguardante una persona fisica identificata o identificabile (detta «interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*"
(**art.4, par. 1 Regolamento UE 2016/679**).

Quali sono i dati personali e le particolari categorie di dati (ex dati sensibili, ma non solo)

I **dati personali** sono un vero e proprio valore, sono tante piccole tessere di un mosaico che compone la **nostra identità**.
I dati personali sono tutte quelle informazioni che ci identificano e descrivono: il nome, il cognome, il luogo dove viviamo, il nostro aspetto, i nostri gusti, i gruppi di cui facciamo parte, la nostra salute.
Tutti noi utilizziamo gli straordinari servizi offerti dalla Rete e non potremmo rinunciarvi. Tali servizi però richiedono l'acquisizione di informazioni contenute nei nostri dati personali. Quindi, più o meno consapevolmente, ogni giorno "doniamo" una piccola parte di noi.
Ma, senza un controllo su come vengono trattati, questi dati potrebbero essere venduti, scambiati, salvati e utilizzati, anche a distanza di anni, per scopi diversi da quelli per cui noi li abbiamo condivisi, con il rischio che possano anche essere usati per danneggiarci.

EX DATI "SENSIBILI"

Il **d.lgs 196/2003** definiva come dati "sensibili": l'origine razziale ed etnica di un individuo, le convinzioni e adesioni religiose, politiche e filosofiche o lo stato di salute e le abitudini sessuali di un soggetto. Questi dati potevano essere trattati solo con il consenso scritto dell'interessato.

L'**art. 9 del GDPR** introduce la definizione di dati "particolari", che va a sovrapporsi e ad ampliare la categoria dei "dati sensibili".
La norma prescrive infatti che: "è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona". Ma il divieto non è assoluto, lo stesso articolo 9 del GDPR indica infatti quali sono le condizioni che permettono il trattamento dei dati particolari.

I dati personali si possono dividere in tre categorie:

- i **dati che permettono l'identificazione diretta**, come i dati anagrafici e le immagini, e **indiretta**, come il codice fiscale, l'indirizzo IP, il numero di targa;

- i **dati rientranti in "categorie particolari"**: tra cui gli **ex dati "sensibili"**, cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose e filosofiche, le opinioni politiche, l'appartenenza sindacale, quelli relativi alla salute o alla vita e l'orientamento sessuale, i dati genetici e biometrici;

IL TRATTAMENTO DEI DATI PERSONALI
è qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali. I soggetti che procedono al trattamento dei dati personali altrui devono adottare particolari misure per garantire il corretto e sicuro utilizzo dei dati.

- i **dati "giudiziari"**, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale, come i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione, o la qualità di imputato o di indagato.

Con l'avanzare delle nuove tecnologie digitali alcune tipologie di dati personali hanno assunto particolare rilevanza. Tra questi:

- i **dati relativi alle comunicazioni elettroniche** via telefono o internet, come ad esempio un indirizzo IP;
- quelli che consentono la **geolocalizzazione della persona**, fornendo informazioni su movimenti e luoghi frequentati;
- i **dati genetici**, che rivelano le informazioni relative alle caratteristiche genetiche di una persona, a seguito dell'analisi di un campione biologico, e i **dati biometrici**, che permettono di individuare una persona, analizzandone le caratteristiche fisiche, fisiologiche o comportamentali.

Tutti dati, questi, facilmente tracciabili da quei dispositivi che indossiamo, come smartband e fitness tracker, o portiamo con noi, come smartphone e tablet.

Le parti in gioco

Interessato

Interessato è la persona fisica alla quale si riferiscono i dati personali. Quindi, se un trattamento riguarda, ad esempio, l'indirizzo, il codice fiscale, ecc. di Mario Rossi, questa persona è l'interessato;

Titolare

Titolare è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione, ecc., che stabilisce scopi e modalità del trattamento;

Responsabile

Responsabile è la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo del trattamento dei dati.

Protezione dei dati personali: tutela il tuo diritto

Alla base della tutela dei nostri dati personali e del rispetto di quelli altrui ci sono la conoscenza dei diritti di cui usufruiamo e la consapevolezza dei rischi che corriamo quotidianamente.
Il **diritto alla protezione dei dati personali** è un **diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8)** e oggi è **tutelato**, in particolare, **dal GPDR**. Quest'ultimo ha ampliato i diritti riconosciuti all'**interessato** con riferimento ai dati che lo riguardano, rendendoli maggiormente incisivi in una realtà in cui si fa sempre più ricorso alle nuove tecnologie e all'utilizzo della rete.

In particolare, questi diritti sono:

- 1 **Diritto di accedere ai propri dati personali**, ovvero il diritto per l'interessato di chiedere al titolare del trattamento se è in corso o meno un trattamento di dati personali che lo riguardano e, qualora il trattamento sia confermato, ottenere una copia di tali dati e tutte le informazioni riguardanti il loro trattamento;

- 2 **Diritto alla rettifica, alla limitazione del trattamento, alla portabilità dei dati personali**. L'interessato può chiedere al titolare che i suoi dati siano rettificati, perché inesatti o non aggiornati, eventualmente integrando informazioni incomplete.
  I dati possono inoltre essere limitati nel relativo trattamento, se non sono esatti o sono trattati illecitamente. Infine, l'interessato può richiedere il trasferimento dei suoi dati a un altro titolare (diritto alla portabilità), se il trattamento si basa sul consenso o su un contratto stipulato con l'interessato e viene effettuato con mezzi automatizzati;

- 3 **Diritto di opposizione**, ovvero il diritto di opporsi al trattamento dei dati personali che lo riguardano per motivi connessi alla sua situazione particolare. L'interessato può opporsi in ogni momento quando i propri dati sono usati per finalità di marketing diretto (cioè quando le imprese inviano ai propri clienti una comunicazione promozionale dei propri beni e servizi senza avvalersi d'intermediari), inclusa la profilazione;

- 4 **Diritto alla cancellazione (diritto all'oblio)**, ovvero per l'interessato il diritto di richiedere la cancellazione dei propri dati personali, se non sono più necessari al perseguimento delle finalità per le quali sono stati raccolti o trattati, se l'interessato revoca il consenso o si oppone al trattamento oppure se i dati sono trattati illecitamente o devono essere cancellati per adempiere a un obbligo legale. I titolari, se hanno "reso pubblici" i dati personali dell'interessato, pubblicandoli ad esempio su un sito web, hanno l'obbligo di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione".
  Ottenendo la cancellazione dei dati, e quindi la loro ulteriore conservazione, l'interessato può essere "dimenticato", da cui il diritto all'oblio.

Tutti noi possiamo esercitare questi diritti al fine di tutelare i nostri dati personali. Per farlo possiamo presentare un'**istanza al titolare del trattamento dei dati**, tramite gli specifici [5] **moduli disponibili sul sito del Garante per la protezione dei dati personali**, con le relative istruzioni per la compilazione e l'invio. Il titolare del trattamento ha 1 mese di tempo per rispondere alla richiesta e deve comunicare un eventuale ritardo nella risposta in caso di richieste numerose e/o complesse (la proroga non può comunque superare i 2 mesi).
Se la risposta non perviene nei tempi indicati o non la ritieniamo soddisfacente, possiamo rivolgerci al Garante per la protezione dei dati personali, mediante un reclamo ai sensi dell'art. 77 del Regolamento, oppure all'autorità giudiziaria.

All'attenzione del Garante

Per portare all'attenzione del Garante eventuali violazioni della normativa in materia di protezione dei dati personali è possibile presentare un reclamo o inviare una segnalazione.

Reclamo

Segnalazione

Link per approfondire:

1. https://www.gpdp.it/home/i-miei-diritti/diritti/diritto-di-accesso
2. https://www.gpdp.it/home/i-miei-diritti/diritti/
3. https://www.gpdp.it/i-miei-diritti/diritto-alla-portabilita-dei-dati
4. https://www.gpdp.it/i-miei-diritti/diritti/oblio
5. https://www.garanteprivacy.it/home/modulistica-e-servizi-online

Suggerimento di attività didattica di cooperative learning:

Al termine della lezione, chiedete ai ragazzi di creare la propria "carta d'identità" dei propri dati personali e di riflettere sui rischi che quotidianamente corrono online.
A seguire, i ragazzi in una sessione di brainstorming potranno confrontarsi e creare un elenco di comportamenti da seguire per tutelare i propri dati personali.

IV.

Sharare, taggare, followare... non siamo mica nabbi

I ragazzi sono sempre un passo avanti, in grado di adeguarsi all'evoluzione ormai inarrestabile delle nuove tecnologie che porta con sé nuove tendenze, nuovi modi di comunicare, nuovi slang. Ma quanto ne sanno su come i social media utilizzano la loro immagine, o sull'età minima per aprire un profilo, quanti conoscono le conseguenze della condivisione di contenuti offensivi e dell'uso improprio delle immagini altrui? Educare i ragazzi all'uso delle nuove tecnologie, distinguendo opportunità e rischi, li aiuterà a comprendere meglio e a tutelare i loro dati e la loro reputazione online.

Reputazione online

La reputazione è la considerazione, la stima, che hanno di noi le persone che ci conoscono. Allo stesso modo, la reputazione online è l'insieme delle opinioni che si formano su di noi le persone che conosciamo, basandosi sulla nostra identità online, per esempio attraverso foto, post e commenti che pubblichiamo o che vengono pubblicati da altri su di noi.

Smartphone: spegni il microfono, accendi la privacy

Ci sono molti aspetti a cui fare attenzione ogni volta che usiamo lo smartphone, il tablet o il computer, come ad esempio:

- le informazioni conservate al loro interno, che potrebbero essere smarrite, rubate o perfino clonate da pirati elettronici;
- i sensori degli smartphone, in particolare il microfono, che spesso restano attivi anche quando non stiamo utilizzando il dispositivo. Potrebbero essere usati per finalità diverse, come raccogliere informazioni su di noi e le nostre abitudini;
- lo spam in posta elettronica, sms o servizi di messaggistica istantanea. Cliccando sui link in essi contenuti potremmo inconsapevolmente accettare di ricevere comunicazioni indesiderate, divenendo bersaglio di messaggi pubblicitari non richiesti, da cui è poi difficile liberarsi;
- le impostazioni di geolocalizzazione dei servizi di social network che comunicano la nostra posizione.

Attenzione!

Molte app al momento dell'installazione richiedono l'accesso al microfono e non tutte garantiscono gli stessi standard di sicurezza e protezione della privacy.
Troppo spesso concediamo questi permessi senza pensarci troppo e senza informarci sufficientemente sull'uso che verrà fatto dei nostri dati.
Chiediamoci: è davvero sempre necessario?

Deepfake: il falso che ti ruba la privacy

I deepfake sono foto, video o audio creati grazie a software di intelligenza artificiale che partono da contenuti reali e li modificano in modo estremamente realistico. Il deepfake può essere utilizzato per attività telematiche illecite, come lo **spoofing** (il furto di informazioni che avviene attraverso la falsificazione di identità di persone o dispositivo, in modo da ingannare altre persone o dispositivi e ottenere la trasmissione di dati), il **phishing** (vedi scheda dedicata) e il **ransomware**. (software che prendono "in ostaggio" un dispositivo elettronico per poi "liberarlo" a fronte del pagamento di somme di denaro). Volti e voci artefatti possono essere utilizzati per ingannare i sistemi di sicurezza basati su dati biometrici vocali e facciali. Ad esempio, video o audio-messaggi deepfake creati da malintenzionati possono essere inviati ai nostri colleghi, amici o parenti per invitarli a cliccare su link o aprire allegati a messaggi che espongono pc, smartphone o altri dispositivi e sistemi a pericolose intrusioni, oppure per convincerli a fornire, ingannando la loro fiducia, informazioni e dati sensibili.

Come possiamo tutelarci

- Non conserviamo su smartphone e tablet informazioni troppo personali, ad esempio, password, codici di accesso e dati bancari in chiaro;
- Ricordiamoci che smartphone e tablet venduti a sconosciuti, regalati o dismessi possono contenere ancora dati personali. Quando ce ne liberiamo ripristiniamo le impostazioni di fabbrica, rimuoviamo la scheda SIM e la scheda di memoria ed eliminiamo tutti i backup contenuti nella memoria;
- Impostiamo sul nostro smartphone sempre un codice PIN complesso, evitando, ad esempio, di usare i nostri nome e cognome, la data di nascita o altre parole che ci renderebbero in qualche modo riconoscibili;
- Impostiamo anche un codice di sblocco, quello che si attiva automaticamente quando il cellulare è acceso ma non viene utilizzato per un po' di tempo. Anche in questo caso, evitiamo codici un po' troppo facili da scoprire;
- Verifichiamo le impostazioni privacy e leggiamo le condizioni d'uso dei siti che navighiamo o delle app che usiamo;
- Scarichiamo le app solo dagli store ufficiali e verifichiamo sempre a quali sensori, funzioni e dati hanno accesso e se è necessario che vi abbiano accesso;
- Per navigare sul web bisogna sempre installare, e tenere aggiornati, i software anti-virus per proteggerci dalle intrusioni dei pirati telematici e dei ladri d'identità digitali;
- Disabilitiamo la geolocalizzazione, il GPS o la connessione wi-fi quando non stiamo usando questi servizi o altri ad essi collegati come la geolocalizzazione dei servizi di social network.

Cyberbulli, no grazie

Il **cyberbullismo** può colpire sempre e ovunque. Una **forma di violenza, prepotenza, oppressione: dal reale al virtuale**. Un fenomeno che preoccupa e che fa leva sulle fragilità dei ragazzi. Paura di essere esclusi e ricerca di ammirazione.
Il cyberbullo ha un pubblico potenzialmente enorme e crede di potersi nascondere dietro l'anonimato. Ciò lo spinge a colpire in modo più aggressivo e violento, generando conseguenze anche gravi.
Non è "solo uno scherzo".
Tutto avviene dietro ad uno schermo, quindi spesso si minimizza l'azione ("ho solo postato un video"). Inoltre, non essendoci vero contatto con la vittima, non si vedono immediatamente gli effetti, il dolore o i danni che l'azione del cyberbullo ha causato sulla vittima.

Legge n.71/2017
Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo.
La legge 71/2017 consente ai minori di chiedere l'oscuramento, la rimozione o il blocco di contenuti a loro riferiti e diffusi per via telematica, che ritengono essere atti di cyberbullismo (ad esempio, foto e video imbarazzanti o offensivi, oppure pagine web o post sui social network in cui si è vittime di minacce, offese o insulti, ecc.).

Modulo per la segnalazione/reclamo in materia di cyberbullismo

Deepfake e cyberbullismo

I video deepfake possono essere creati ad hoc per realizzare veri e propri atti di cyberbullismo, che hanno come vittime soprattutto giovani. Un deepfake può essere realizzato per denigrare, irridere e screditare le persone coinvolte, o addirittura per ricattarle, chiedendo soldi o altro in cambio della mancata diffusione del video oppure per la sua cancellazione se è già stato diffuso.

Come possiamo tutelarci

- Cerchiamo di non reagire, comportandoci allo stesso modo del cyberbullo, non rispondiamo ai messaggi provocatori e blocchiamo i contatti;
- Teniamo traccia di ciò che accade online: messaggi e provocazioni ricevuti possono essere prove della violenza a cui si è stati sottoposti;
- Sui social e sui siti web segnaliamo i contenuti e l'autore del messaggio provocatorio, inoltre limitiamo la privacy dei contenuti che condividiamo online;
- Richiediamo alle piattaforme e alle autorità (Polizia postale e Garante privacy) la cancellazione di contenuti che ci riguardano.

Stop a sexting e revenge porn

Nel caso del **sexting** e **revenge porn** ad essere **condivisi online sono contenuti sessualmente espliciti, senza il consenso della persona interessata, con lo scopo di vendicarsi, bullizzare, molestare o denigrare pubblicamente**. È facile immaginare gli effetti drammatici che possono avere a livello psicologico, sociale e anche materiale sulla vita delle persone che ne sono vittime. Diventa quindi fondamentale sapere come difendersi e prevenire questo tipo di fenomeni, attraverso una corretta protezione e gestione dei nostri dati personali e in particolare di messaggi, foto e video che ci ritraggono.

Attenzione!
Una volta che un'immagine o un video sono fissati su un supporto digitale ne perdiamo il controllo.
Si può limitarne la diffusione, ma non abbiamo la garanzia che "quel" video potrà essere di nuovo riportato nella sfera intima e privata alla quale era destinato.

Deepnude

L'intelligenza artificiale può purtroppo facilitare le azioni di revenge porn tramite il cosiddetto deepnude, una pericolosa variante del deepfake. Partendo da foto o video reali del tutto "normali", che riprendono ad esempio il soggetto in comuni situazioni e attività di vita quotidiana, si possono manipolare le immagini "denudando" le persone e/o rappresentandole in pose o azioni esplicitamente sessuali false ma del tutto realistiche.

Come possiamo tutelarci

- Proteggiamo sempre i nostri dati: se nei nostri dispositivi conserviamo foto o filmati intimi, usiamo adeguate misure di sicurezza (es. password, sistemi di crittografia o antivirus);
- Diventiamo consapevoli: se decidiamo di diffondere le nostre immagini tramite messaggi o social, anche se il nostro profilo è "chiuso", i nostri contenuti potrebbero essere condivisi da altri e ne perderemo il controllo. Inoltre, ricordiamoci che la tecnologia è in grado di manipolare le immagini;
- Far cancellare dati che ci riguardano è un nostro diritto; chiediamo a chi è in possesso di immagini esplicite che ci riguardano di cancellarle per bloccare ogni possibilità di ulteriore diffusione;
- La prima difesa è la prudenza: cerchiamo sempre di limitare la diffusione di ogni tipo di foto e immagini personali tramite messaggistica e social network;
- Non aiutiamo il revenge porn: se riceviamo foto o immagini che potrebbero essere frutto di revenge porn non diffondiamole, cancelliamole e, se riteniamo, facciamo una segnalazione alla Polizia postale o al Garante;
- Prestiamo molta attenzione anche all'utilizzo delle app di dating online.

Social privacy: niente è gratis

I social network sono piazze virtuali in cui ci si ritrova, si condividono fotografie, filmati, pensieri, vita.
Uno straordinario strumento di comunicazione che accorcia le distanze e ci dona l'impressione di avere uno spazio personale e riservato.
È proprio questo senso di intimità che può spingerci ad **esporre troppo la nostra vita privata**, rivelare informazioni confidenziali o pubblicare foto con troppa leggerezza.

Quando inseriamo i nostri dati personali su un social ne perdiamo il controllo, concedendo al fornitore la possibilità di utilizzare per un tempo indefinito il materiale che postiamo (foto, chat, post scritti, etc).

Falsa intimità

Spesso è lo stesso termine di "community" a falsare la prospettiva: non sappiamo mai qual è veramente la nostra platea. Quando siamo nel mondo fisico possiamo vedere chi ascolta le nostre conversazioni, chi ci guarda. Nel mondo Internet le nostre informazioni si disseminano e non ne abbiamo più il controllo.

"Gratis" non sempre significa "a costo zero"

Le aziende che gestiscono i social network si finanziano vendendo pubblicità mirate.
Il valore di queste imprese è legato proprio alla loro capacità di analizzare nel dettaglio i profili degli utenti: abitudini, hobby, interessi, condizioni di salute, orientamento politico o sessuale, rete di contatti etc.
Tutto ciò al fine di prevedere i nostri acquisti, le nostre scelte ed i nostri comportamenti.
Queste informazioni vengono poi vendute a chi sceglie di utilizzare i social per promuovere la propria attività, lanciare offerte commerciali o sostenere campagne di diverso genere.
Sui social e sul web in generale dietro ad un servizio gratuito si nasconde lo sfruttamento dei nostri dati.

Attenzione all'identità

Non sempre parliamo, chattiamo e condividiamo informazioni con chi crediamo.
Possiamo trovarci a "dialogare" con falsi profili, creati grazie a un bot che simula azioni umane.
Tali profili sono creati per scopri precisi: furto di informazioni personali, commettere truffe o danneggiare.

Come possiamo tutelarci

- Quando postiamo una foto di un nostro amico o familiare taggandolo, domandiamoci se stiamo violando la sua privacy e nel dubbio chiediamo prima il consenso. Privacy è rispetto per sé stessi e per gli altri;
- Controlliamo chi può vedere le nostre immagini. Nelle amicizie esistono diversi livelli di relazione: mostrerei la stessa foto al mio amico e alla mia prof? Mostrerei "quella foto" con l'ex anche al mio nuovo ragazzo / la mia nuova ragazza?;
- Controlliamo i tag associati al nostro nome su foto e video;
- Controlliamo i livelli di privacy sul nostro profilo: chi ci può contattare, chi può leggere quello che scriviamo, chi può inserire commenti nelle nostre pagine, che diritti hanno gli utenti dei gruppi ai quali apparteniamo;
- Limitiamo al massimo la disponibilità di informazioni, soprattutto per quanto riguarda la reperibilità dei dati da parte dei motori di ricerca;
- Controlliamo quali diritti di accesso concediamo alle App che installiamo sullo smartphone o sul tablet affinché non possano utilizzare i nostri dati personali (contatti, telefonate, foto...) senza consenso;
- Se non desideriamo ricevere pubblicità, ricordiamoci che possiamo rifiutare il consenso all'utilizzo dei dati per attività mirate di promozione e marketing;
- Utilizzare messaggi che si "autodistruggono" dopo la lettura non mette a riparo dai rischi di un uso inappropriato del materiale condiviso. Ricordiamo che tutto ciò che condividiamo può sempre essere salvato e riutilizzato;
- Facciamo sempre attenzione a ciò che facciamo online e alle informazioni che condividiamo, perché potrebbe avere effetti anche sulla nostra vita reale;
- Se notiamo comportamenti anomali e fastidiosi su un social network, se vediamo che un nostro amico è insultato e messo sotto pressione da individui o gruppi, non aspettiamo e segnaliamo subito la situazione critica al gestore del servizio affinché possa intervenire immediatamente. In caso di violazioni, segnaliamo subito il problema al Garante e alle altre autorità competenti. Se invece siamo noi stessi vittima di odiosi commenti a sfondo sessuale, di cyberbullismo o di sexting, se stanno violando la nostra privacy, non aspettiamo che la situazione degeneri ulteriormente e chiediamo aiuto alle persone care e, anche in questo caso, al Garante e alle autorità competenti.

Suggerimento di attività didattica di role playing:

Al termine della lezione, chiedete ai ragazzi di dividersi in gruppi e di pensare a una delle situazioni di rischio trattate in cui si sono ritrovati. Ad ogni studente sarà poi assegnato un ruolo, in base alla situazione descritta, e in gruppo dovranno ragionare e confrontarsi per mettere in pratica le azioni consigliate per affrontare la situazione di rischio e trovare insieme delle regole per evitarle.

V.

I termini della Rete

Il linguaggio moderno non può non essere influenzato dal mondo del web e dei social media, che hanno creato espressioni linguistiche nuove, frutto di contaminazioni e slang.
Parliamo di neologismi, parole inglesi o che derivano dal "gergo" social che ormai fanno parte della quotidianità.

Assistenti digitali

Programma in grado di dialogare con gli esseri umani tramite algoritmi di intelligenza artificiale. L'assistente digitale (smart assistant) riesce a rispondere a richieste di informazioni, fare ricerche su internet, dare indicazioni stradali, fare acquisti online, regolare la temperatura o l'illuminazione di un'abitazione, etc. Troviamo questa tecnologia sugli smartphone ma anche a casa o in macchina. Gli smart assistant possono raccogliere e memorizzare una grande quantità di dati personali, non solo relativi all'utilizzatore diretto, ma a chiunque si trovi nello stesso ambiente: scelte, preferenze, abitudini di consumo, caratteristiche biometriche, stati emotivi, percorsi abituali che percorriamo, indirizzi.

Per approfondire

Cookie

I cookie sono piccoli file di testo che i siti web visitati da un utente inviano al dispositivo utilizzati per navigare in rete (computer smartphone, tablet, smart TV, etc.). Dal punto di vista operativo, servono a velocizzare e semplificare la fruizione dei siti web: permettono infatti di tenere traccia della nostra attività su un sito specifico, memorizzando per esempio articoli inseriti temporaneamente in un carrello o informazioni digitate in un modulo on line. Ma i cookie possono anche veicolare la pubblicità comportamentale, in funzione delle nostre abitudini e preferenze di navigazione, e misurare poi l'efficacia del messaggio pubblicitario.

Per approfondire

Deepfake

Fusione di "fake" (falso) e "deep learning" (particolare tecnologia AI). Foto, video e audio creati grazie a software di intelligenza artificiale che, partendo da contenuti reali, riescono a modificare o ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o un corpo e a imitare fedelmente una determinata voce. Quella realizzata con i deepfake è una forma particolarmente grave di furto di identità. Le persone che compaiono a loro insaputa in un deepfake non solo subiscono una perdita di controllo sulla loro immagine, ma sono private anche del controllo sulle loro idee e sui loro pensieri.

Per approfondire

Deepnude

Una forma particolare di deepfake in cui persone ignare possono essere rappresentate nude, in situazioni compromettenti o in contesti pornografici. Con questa tecnologia i visi delle persone possono essere innestati sui corpi di altri soggetti, nudi o in pose o atti di natura esplicitamente sessuale. Inizialmente il fenomeno ha coinvolto personaggi famosi allo scopo di screditarli o ricattarli. Ma negli ultimi tempi, con la maggiore diffusione di software che utilizzano questa tecnologia, il rischio coinvolge anche persone comuni, le quali possono diventare oggetto di azioni psicologicamente e socialmente molto dannose.

Per approfondire

Dating online

Siti o app di incontri online che permettono di creare un profilo e cercare un partner con l'aiuto di un algoritmo. Come gli altri social network si tratta di piattaforme gestite da società a scopo di lucro, quindi possono raccogliere, trattare e diffondere le informazioni. È importante fornire solo i dati indispensabili per la fruizione del servizio e riflettere bene prima di caricare foto e video personali.

Per approfondire

Giocattoli intelligenti

Giocattoli come bambole, peluche, robot e giochi educativi, in grado di interagire con le persone e con l'ambiente circostante attraverso microfoni, fotocamere, sistemi di localizzazione e sensori. Gli smart toys si connettono alla rete per navigare e compiere automaticamente varie operazioni come registrare suoni, scattare foto, girare video e collegarsi con web e social network. Si tratta dunque di strumenti che raccolgono, elaborano e comunicano dati e informazioni, con possibili rischi per la privacy, soprattutto quella dei minori.

Per approfondire

Dispositivi indossabili

Dispositivi indossabili a contatto con il corpo come i popolari smartwatch, ma anche braccialetti, visori per la realtà aumentata etc. Questi dispositivi, apparentemente innocui, possono indurci a sottovalutarne i rischi, dovuti alla capacità di rivelare, mediante l'uso secondario dei dati raccolti, stili di vita, patologie, vulnerabilità e dipendenze. I dati sanitari che questi dispositivi possono acquisire possono esporci a forme di discriminazione, rivelare le nostre reazioni emotive, quindi attingere al nostro pensiero.

Per approfondire

Phishing

Il phishing deve il suo nome a una variazione del verbo inglese fishing (pescare) operata in ambito informatico. Si tratta di tecnica illecita utilizzata per appropriarsi di informazioni riservate (username e password, codici di accesso, PIN, numeri di conto corrente, dati del bancomat e della carta di credito), con l'intento di compiere operazioni fraudolente. La truffa avviene di solito via e-mail, ma possono essere utilizzati anche sms, chat e social media. I messaggi di phishing invitano a fornire direttamente i propri dati personali, oppure a cliccare un link che rimanda ad una pagina web dove è presente un form da compilare. I dati così carpiti possono poi essere utilizzati per fare acquisti a spese della vittima, prelevare denaro dal suo conto o addirittura per compiere attività illecite utilizzando il suo nome e le sue credenziali.

Per approfondire

VI.

Il Garante della Privacy

Il Garante per la protezione dei dati personali è un'Autorità indipendente, istituita per assicurare la tutela dei diritti e delle libertà fondamentali nel trattamento dei dati personali e il rispetto della dignità degli individui. Ha iniziato la sua attività nel **1997**, con l'**entrata in vigore della legge sulla privacy (legge 31 dicembre 1996, n.675)**, normativa disciplinata in seguito dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003 n. 196). Con il **Decreto legislativo 10 agosto 2018 n.101**, il Garante è stato **confermato come autorità di controllo designata anche ai fini dell'attuazione del Regolamento generale sulla protezione dei dati personali (UE) 2016/679 (art. 51)**. Il Garante è un organo collegiale, composto da quattro membri eletti direttamente dal Parlamento, i quali rimangono in carica per un mandato di sette anni non rinnovabile. L'attuale Collegio, **presieduto dal Prof. Pasquale Stanzione,** si è insediato nel luglio 2020.

I compiti del Garante

Come definito dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs 196/2003), il Garante si occupa tra l'altro di:

- Controllare che il trattamento dei dati personali da parte di privati e pubbliche amministrazioni sia conforme al Regolamento e alla normativa nazionale;
- Prescrivere ai titolari o ai responsabili dei trattamenti le misure da adottare per svolgere correttamente il trattamento nel rispetto dei diritti e delle libertà fondamentali degli individui;
- Esaminare i reclami;
- In caso di violazione, rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento e ingiungere di conformare i trattamenti alle disposizioni del Regolamento; imporre una limitazione provvisoria o definitiva del trattamento, incluso il divieto di trattamento; ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento;
- Adottare i provvedimenti previsti dalla normativa in materia di protezione dei dati personali e applicare sanzioni pecuniarie, quando previsto dal Regolamento;
- Collaborare con le altre autorità di controllo (i Garanti degli altri Paesi Ue) e partecipare alle attività dell'Unione europea ed internazionali di settore;
- Segnalare, anche di propria iniziativa, al Parlamento e altri organismi e istituzioni l'esigenza di adottare atti normativi e amministrativi relativi alle questioni riguardanti la protezione dei dati personali;
- Predisporre una relazione annuale sull'attività svolta e sullo stato di attuazione della normativa sulla privacy da trasmettere al Parlamento e al Governo;

- Formulare pareri su proposte di atti normativi e amministrativi e partecipare alla discussione su iniziative normative con audizioni presso il Parlamento;
- Curare l'informazione e sviluppare la consapevolezza del pubblico e dei titolari del trattamento in materia di protezione dei dati personali, con particolare attenzione alla tutela dei minori;
- Coinvolgere, ove previsto, i cittadini e tutti i soggetti interessati con consultazioni pubbliche dei cui risultati si tiene conto per la predisposizione di provvedimenti a carattere generale.

Cultura della consapevolezza

Sia adulti che adolescenti spesso non hanno una piena percezione degli elevati rischi ai quali si espongono utilizzando dispositivi connessi alla Rete, app e social network. Per questo motivo uno degli obiettivi del Garante della Privacy è quello di promuovere attività di sensibilizzazione che riescano a favorire la comprensione dei rischi ma anche degli strumenti di tutela in materia di protezione dei dati personali.
Con la Legge 20 agosto 2019, n. 92 è stato introdotto nelle scuole di ogni ordine e grado, l'insegnamento dell'Educazione Civica e nell'ambito della materia si inserisce proprio la "Cittadinanza digitale"; con l'obiettivo di fare in modo che le ragazze e i ragazzi, fin da piccoli, possano imparare principi come il rispetto dell'altro e dell'ambiente che li circonda, utilizzino linguaggi e comportamenti appropriati quando sono sui social media o navigano in rete. Partendo dalla scuola e attraverso progetti formativi, workshop, seminari, convegni e eventi di approfondimento, il Garante si pone l'obiettivo di formare e consolidare una cultura della consapevolezza.

Il Garante a supporto delle scuole

Il Garante per la protezione dei dati personali è intervenuto con apposite FAQ dedicate alle scuole, per rispondere ad alcuni dubbi frequenti.

VII.

Diventa Ambasciatore della Privacy

Il Contest

Attraverso il contest creativo **Diventa Ambasciatore della Privacy**, il **Garante per la protezione dei dati personali** invita tutti gli studenti delle **classi I e II degli istituti aderenti all'iniziativa** alla realizzazione di **un video**, nelle forme tipiche del linguaggio dei social network, **finalizzato a sensibilizzare i loro coetanei sulla tutela della privacy e dei dati personali**.

In un'ottica di **apprendimento attivo**, gli studenti, con il **supporto di voi docenti**, avranno l'opportunità di **mettere in pratica quanto appreso** durante le lezioni in classe e di poter **trasmettere il valore del rispetto della nostra privacy e di quella altrui e l'importanza di un uso consapevole della Rete e delle nuove tecnologie**.

I video realizzati dovranno essere inviati tramite caricamento nell'apposita sezione dedicata sul Sito ambasciatoriprivacy.it/, a cura del docente registrato, entro e non oltre il **15/04/2023**.

Possono partecipare fino a **3 video per istituto**.

I **3 video selezionati** tra tutti quelli ammessi in graduatoria **dalla Commissione del Garante per la protezione dei dati personali** riceveranno:

al **1° classificato**: un premio di **€3.000 per acquisti di strumenti tecnologici**;
al **2° classificato**: un premio di **€1.500 per acquisti di strumenti tecnologici**;
al **3° classificato**: un premio di **€1.000 per acquisti di strumenti tecnologici**.

La data della premiazione verrà comunicato sul sito www.gpdp.it/ambasciatoriprivacy e sul sito ambasciatoriprivacy.it

Linee guida

Gli studenti dovranno produrre **un video inedito, autoprodotto e originale** per sensibilizzare i loro coetanei **sul valore dei dati personali, sull'importanza di proteggerli e di conoscere gli strumenti per farlo**, sviluppando uno o più temi tra quelli oggetto dell'iniziativa:

Temi oggetto dell'iniziativa

- Il valore dei dati personali e l'importanza di proteggerli;
- Il rapporto tra la protezione dei dati le nuove tecnologie e i giovani, con particolare riferimento all'uso dei dispositivi e delle app;
- Furti d'identità online;
- Cyberbullismo;
- Sexting;
- Revenge Porn;
- Phishing;
- Deepfake;
- Deepnude;
- Profilazione degli utenti da parte delle grandi piattaforme.

Il video dovrà utilizzare un linguaggio adatto ai social network, con lo scopo di raggiungere nell'immediato un pubblico di pari età e farlo interagire in modo attivo, educandolo e coinvolgendolo, e dovrà avere i seguenti requisiti:

Requisiti del video

- essere in formato orizzontale 16:9 o verticale 9:16
- durare non più di 60";
- avere dimensioni non superiori a 200 Mb;
- stile "video infografica"
- contenere immagini e sequenze filmate inedite;
- utilizzare, se previste, tracce sonore presenti nelle librerie gratuite indicate dal regolamento.

Per stile "video infografica", si intende una combinazione di immagini, statiche o dinamiche, accompagnate a testi, suoni senza prevedere il coinvolgimento di attori interpretati da persone fisiche filmate e/o audio registrate direttamente dagli autori del video.
Sono quindi ammessi video con i seguenti elementi visivi:

Elementi visivi ammessi

- motion graphics, ovvero video grafiche animate di ogni genere;
- fumetti, vignette e/o cartoni animati;
- testi e grafici statici o animati in sovraimpressione.

I video realizzati verranno utilizzati dal Garante a fini di divulgazione e promozione della cultura della privacy. Per partecipare al concorso è quindi necessario far firmare alla scuola una liberatoria presente nell'area riservata del sito ambasciatoriprivacy.it.

Consigli utili per la realizzazione del video:

Identificare l'obiettivo e un messaggio unico: il primo passo per la buona riuscita del video è organizzare un **brainstorming**, in cui gli studenti si confrontino e in base a quello che hanno appreso e alle loro esperienze personali decidano insieme la tematica secondo loro fondamentale da trattare nel video;

Storytelling: è importante individuare i punti chiave del loro progetto e raccontarlo in modo chiaro con parole semplici e senza troppi filtri;

Storyboard: produrre delle miniature di fotogrammi e scene che si desidera inserire nel video, insieme a note per ciascuno di essi, può essere utile a delineare visivamente il video;

Call to action: inserire una call to action può essere utile a dare più concretezza al loro obiettivo e coinvolgere in maniera più attiva chi guarderà il video.

Qualora si vogliano apportare delle correzioni o migliorie al video, **si potrà sostituire il video fino alle 23:59 del 15/04/2023**.

Per la partecipazione al contest creativo potete consultare il regolamento e tutti i documenti necessari per la realizzazione del video e la sua validità sul sito dedicato ambasciatoriprivacy.it.

Ora tocca ai vostri ragazzi diventare Ambasciatori della Privacy!

Buon lavoro e un grosso in bocca al lupo a tutte le classi partecipanti!

Diventa ambasciatore della privacy

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Con il supporto tecnico di

SKUOLA.net