



DigitalRightsFoundation
"KNOW YOUR RIGHTS"

GUIDEBOOK ON DATA PRIVACY



Supported by



**FRIEDRICH NAUMANN
FOUNDATION** For Freedom.

Pakistan

About Us

Digital Rights Foundation (DRF) is a registered research-based advocacy non-governmental organization in Pakistan. Founded in 2012, DRF focuses on ICTs to support human rights, inclusiveness, democratic processes, and digital governance. DRF works on issues of online free speech, privacy, data protection and online violence against women. DRF opposes any and all sorts of online censorship and violations of human rights both on-ground and online.

For more information visit:

www.digitalrightsfoundation.pk



DigitalRightsFoundation
"KNOW YOUR RIGHTS"



Supported by

**FRIEDRICH NAUMANN
FOUNDATION** For Freedom.

Pakistan

Disclaimer

Every effort has been made to ensure the accuracy of the contents of this publication. The authors or the organization do not accept any responsibility of any omission as it is not deliberate. Nevertheless, we will appreciate provision of accurate information to improve our work. The views expressed in this report do not necessarily represent the views of the Friedrich Naumann Foundation for Freedom. The content of the publication is Digital Rights Foundation's responsibility.

Contents

Context	1
Aims And Objectives	3
Summary	4
Children's Section	5
What Is Data?	6
What Is Privacy?	7
What Is Consent?	9
Age Of Majority And Minority	10
Social Media for Minors	11
Difference Between The Private And Public Sphere	12
What Is Private Data?	13
Who are data collectors and holders?	14
Why is data protection important?	15
Autonomy	16
Right To Stay Anonymous	17
The Implications Of Your Digital Identity	18
What To Share And What Not To Share?	20
Practical	21
How To Safeguard Your Data?	22
Secure your device	22
Protect against viruses and malware	23
Backup	24
Up your password game	24

Two-factor authentication _____	26
Browser security _____	27
Browser add-ons _____	28
How To Keep Your Social Media Secure And Anonymous ____	29
Vpn_____	31
Gps_____	32
Understand Cyber-Harassment _____	33
What To Do When There Is A Privacy Breach? _____	35
How Can Your Data Be Used Against You? _____	36
Parents _____	37
Protect your child's privacy on your own social media_____	42
Privacy does not mean secrecy _____	43
Set a good example _____	44
Resources _____	45

Context

According to the United Nations Convention on the Rights of the Child, children are not just objects who belong to their parents and for whom decisions are made, or young adults in training. Instead, they are human beings and individuals with their own rights¹.

The convention makes a distinction between childhood and adulthood, with the former lasting until 18 years of age. It is a legally protected and socially recognised time in which children must be allowed to grow, learn, play, develop and flourish with dignity. Unicef recognises that the rise of digital technology is one of the phenomena that have changed what childhood means today. According to Unicef, today's children face new threats to their rights, but they also have new opportunities to realise their rights².

The internet is a vast space used by many people across the globe for various purposes. It is also very fascinating for children, given that they are exploring everything in life. The internet provides you with knowledge, entertainment and also keeps you connected to multiple users across the globe. The use of the internet has integrated the global community even more. However, the use of the internet has a dark side, too. When people use the internet, they end up sharing their data with users and companies across

1 "What is the Convention on the Rights of the Child?", Unicef, <https://www.unicef.org/child-rights-convention/what-is-the-convention>

2 ibid

be collected for various purposes. Users across the globe are like data factories - they generate data and post it on the web everyday. In turn, this data is used and analysed in a manner that behavioural patterns of internet users across the globe can be predicted.

Internet users in Pakistan are also data factories for the country - they are generating data and patterns for companies to analyse. Companies use this data to make their services better and to predict upcoming market trends. However, there are companies that use this data for unethical purposes and they sometimes end up selling this data to third parties without the consent of the user.

In this scenario, it is particularly important that children are equipped with the tools to protect their own privacy. Parents should also help uplift their children in this regard instead of imposing sweeping restrictions on the use of digital technology altogether. We embrace the right of the child to exist in their own right, as laid down in the United Nations Convention on the Rights of the Child, and this data privacy booklet aimed at children is a contribution in that direction.

Aims and objectives

Through this booklet, we aim to equip children and youth with the necessary tools that enable them to protect their privacy in the digital world. In an age when even adults are not safe from the dark side of the digital world, it is particularly important that we come up with measures to protect children and young adults from potential misuse and abuse of data.



Summary

We have attempted to explain in simple language what data is, what privacy is, what data protection means and why these are important. We have also tried to elaborate on the distinction between the public and private spheres, and also how one's data can be used against them. Finally, we have given tips for safeguarding your data.

Our section on parents tries to explain the role and duty of parents and/or legal guardians towards enabling their children to safeguard their data. Our approach is rooted in the idea that parents do not own their children and, hence, should take responsibility instead of control over their children's protection.



CHILDREN'S SECTION



What is data?

Data is information. Your data is your information. No one without your permission has the right to access or disclose your data, unless it is a matter of safety or legal proceedings by an authorised person, i.e. legal guardian, police or courts.

Your name, home address, phone number, school's name, photos or any other information that could be used to identify you is your personal data.



What is privacy?

Privacy is freedom from all kinds of interference or intrusions. Information privacy, in particular, is the right to have some control over how your personal information is collected and used³. It is a fundamental human right that everyone has, regardless of their class, race, age, gender or any other identity marker.

According to Privacy International, privacy is one right that serves as the foundation upon which many other human rights are built⁴. This is precisely what makes it so important.

The right to privacy enables us to draw our own boundaries and determine who we would like to interact with. It serves as a barrier that protects us from unwarranted interference. According to the Office of the Australian Information Commissioner, the right to privacy generally entails the right a. to be free from interference and intrusion, b. to associate freely with whom you want, and c. to be able to control who can see or use information about you⁵.

Therefore, the right to privacy protects you from being asked to volunteer information about yourself. No one has the right to demand that you share your photos, home address or school's name with them unless it is a

3 "What does privacy mean?", IAPP, <https://iapp.org/about/what-is-privacy/>

4 "What is Privacy?", Privacy International, <https://privacyinternational.org/explainer/56/what-privacy>

5 "What is Privacy?", Office of the Australian Information Commissioner, <https://www.oaic.gov.au/privacy/your-privacy-rights/what-is-privacy/>

matter of safety or legal proceedings by an authorised person, i.e. legal guardian, police or courts. Similarly, companies do not have the right to collect your data, such as your location and gender among other things, without your consent.

It's okay to want privacy—you're not hiding anything. You don't have to be a tech expert to protect your privacy either!



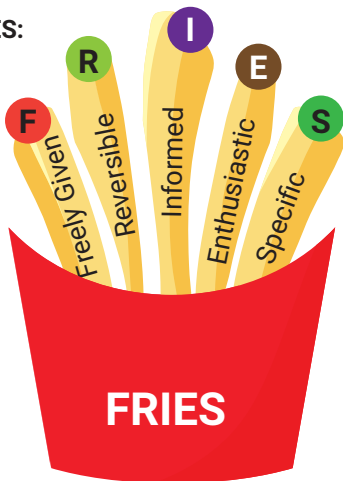
What is consent?



TIP: Ask for permission before you take a picture.

Your consent, i.e. informed agreement, is required before someone can use your data. For example, people should ask you before they take photographs of you. Similarly, your consent is required for processing your data. For example, if you use Facebook, the social networking platform requires your consent to use your data for business purposes. If you are still a minor, one of your parents is required to give consent on your behalf about usage of your data.

Consent is FRIES:



Age of majority and minority

Once you turn 18, you are of an age to give your consent. Until then, you have limited consent, i.e. your parents or guardian will be responsible for some of this decision-making.

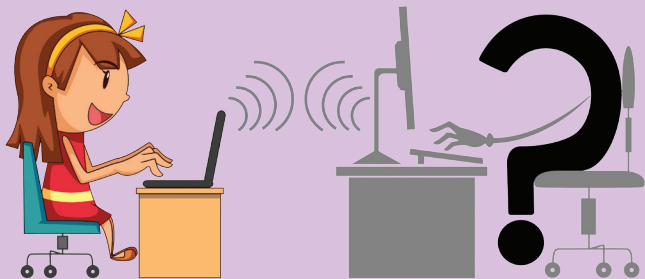
However this does not mean that you have no privacy rights over your parents or guardian: it is important to educate adults about the importance of respecting the privacy of children and young adults.



Social media for minors

You should not lie about your age on social media. Social media websites protect you in some ways from potential misuse of data as minors. When you lie about your age, you lose that protection and leave your data vulnerable to misuse.

On some social media websites, minors below the age of 13 cannot make social media accounts.



Difference between the private and public sphere

Your home is your private sphere. No one has the right to encroach upon your private sphere without your permission. The public sphere is what lies outside of homes. For example, the playground in your neighbourhood park is a public space. Similarly, hospitals and streets are public spaces. We behave differently in public and private spheres. In the public sphere, we are more cautious of how we appear and how we talk and interact with others. By contrast, the private sphere is your comfort zone. You are not answerable to anyone about it. For example, you can roam around in your home without brushing your hair. But you would not go out like that.

The digital sphere also has a public-private distinction. Your Facebook profile is your private domain and you have the right to control part of what you share and with whom you share. In short, you can exercise some control over your online data. For example, Facebook allows you to control with whom you will share your year of birth. However, your name and profile photo will be visible to anyone on Facebook - unless you have blocked them.

Therefore, just like your offline identity, you also have an online identity. It is important to bear in mind the similarities and differences between the two as it can help you protect your data in a more effective manner.

What is private data?

Private data is information that is personal, i.e. information that can be used to identify you. Your name, photos, home address, school's name, phone number, etc. are all examples of private data. No one has the right to demand this data from you unless there is authorisation by law enforcement or a court.



Who are data collectors and holders?

Your data is being collected, processed and stored by several actors through digital means. When you visit a website, browsing data is generated and collected regarding what you visited, how much time you spent there and what you clicked on. Anyone who collects, stores or analyses your browsing data is a **data collector**.

It is important to know that data collectors can be your (or other countries') governments, private companies such as Facebook, TikTok or Twitter, or those around you. These are data collectors that collect data through legal means. But some people use illegal means, such as hacks or data leaks, to collect data.

Data holders are persons or organisations who either store your data or your data has been shared with them. Data holders can be both data collectors or third parties with whom your personal information is shared.



Why is data protection important?

Technological advancement results in all the more progress in the digital domain. However, it also means that technology bears the potential of becoming increasingly invasive.

It is important to have private information as it allows you to have agency over your data. With technology becoming ever more invasive, the threat of data being compromised also increases. Therefore, it is important to ensure that your data is protected. Recent examples of data breaches, such as the one at NADRA and Safe City project, have brought into light the various ways in which citizens' data can be compromised and misused.



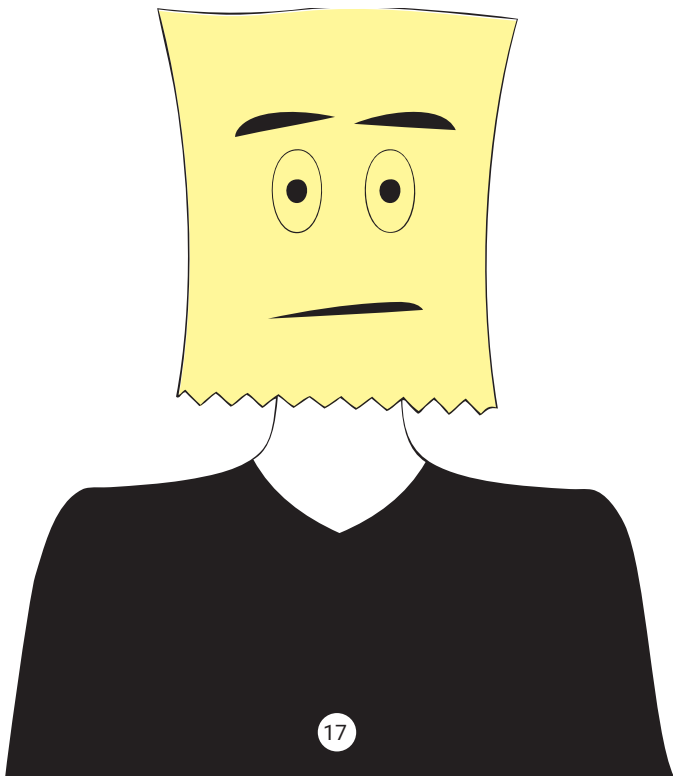
Autonomy

Just like you have autonomy over your body, i.e. the right to control access to it, you also have autonomy over your data. This means that you are entitled to control what you share in online spaces and also with whom. You can control your privacy settings to restrict access of your data to specific people. For example, Facebook allows you to control the privacy of every post that you put up online. You can share it with everyone, just your friends, or selected friends by customising your friend list audience.



Right to stay anonymous

You have a right to stay anonymous. To maintain anonymity, you can prevent users from looking you up through your email address or phone number. You can also prevent users from sending you messages by controlling your privacy settings.



The implications of your digital identity

Some people are under the impression that what they delete from social media is gone forever. That is not true. Even if a website gets deleted, there will be an online cache that will have those website entries still available. Nothing is, hence, really private once it is shared online.

You should, therefore, be careful about the information you put up about yourself. And this is one important reason why you should keep searching your name on Google - it is not narcissistic but a protective measure. You never know which friend from years ago that you trusted on social media has shared your personal information on different platforms online.

In fact, a lot of parents these days set up social media profiles for their children even before they are born. They share photos and other information about the child. This deprives the child of the opportunity to even consent before their data is put up. Therefore, keep checking online what your parents or other relatives may have potentially posted about you online!



Similarly, everything that you do online leaves a digital footprint, i.e. an impression of who you are. This information is collected by websites and can be used to identify, track or even commodify you. Companies will sell this data to advertisers to make huge profits. All your favourite social media platforms such as Facebook, Instagram, TikTok do it.⁶ The agreement that Facebook makes with you includes terms and conditions that allow Facebook to collect information about you because that is mainly how it makes money.



6 <https://www.theguardian.com/technology/2019/jul/02/tiktok-under-investigation-over-child-data-use>
<https://www.theatlantic.com/technology/archive/2018/12/facebooks-failures-and-also-its-problems-leaking-data/578599/>

What to share and what not to share?

In order to determine what you should and should not share on social media, you should think about the distinction between the public and private sphere. Just don't share online what you wouldn't share in offline spaces. For example, do you stand on the streets and distribute print-outs of your personal photos to random passers-by? If you don't, then why should you circulate your personal photos in the digital sphere?

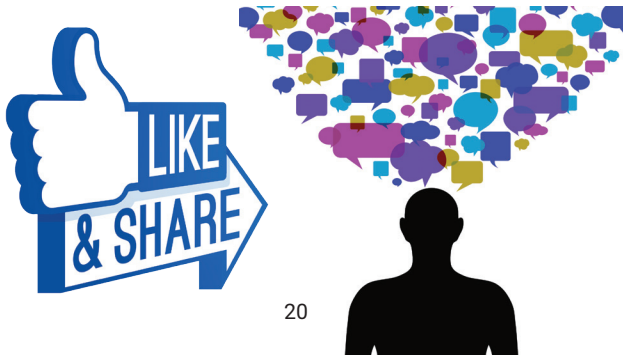
Before posting something online, ask yourself:

✓ could someone use this information to harm me?

✓ will I regret if someone shared this information about me with others?

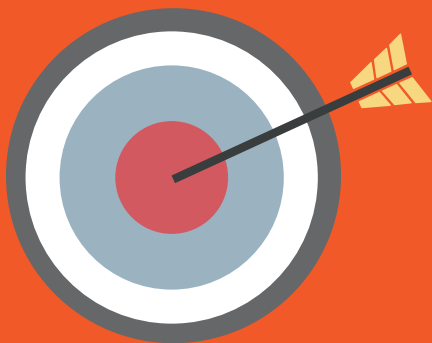
✓ would I share this with people offline?

It is important to think about these questions to make a decision on whether or not you should share some of your information online.






PRACTICAL



How to safeguard your data?

In order to determine what you should and should not share on social media, you should think about the distinction between the public and private sphere. Just don't share online what you wouldn't share in offline spaces. For example, do you stand on the streets and distribute print-outs of your personal photos to random passers-by? If you don't, then why should you circulate your personal photos in the digital sphere?

Before posting something online, ask yourself:



could someone
use this
information to
harm me?

will I regret if
someone shared
this information
about me with
others?

would I share
this with people
offline?

It is important to think about these questions to make a decision on whether or not you should share some of your information online.

Secure your device

If you own a device, whether it is a computer, mobile phone or tablet, you should have a security code. A password or passcode will ensure that your device is protected when left unattended and even in case it gets lost or stolen.

Protect against viruses and malware

Malware is the short form of “malicious software”. Such software can harm your computer system. Remember, all viruses are malware but not all malware are viruses. Professional criminals and hackers across the world are developing different kinds of malware to infect your computer and spy on you, for example, through stealing your banking information. Therefore, you should have anti-virus software along with anti-malware software to protect your device. You can use Avast, AVG, Avira, Kaspersky and Norton Anti-virus software against viruses and Malwarebytes, Lavasoft and Spybot against malware.



BEWARE! We caution against borrowing a USB drive or allowing someone to use yours. Sometimes, people will deliberately install malware on their USB drive to infect a target's computer.



TIP: Run the USB through anti-virus and anti-malware software every time you use it.

 **McAfee™**



Norton
by Symantec



LifeLock

Malwarebytes

 **avast**

Backup

Has your computer ever crashed when you had your presentation saved in it? Losing data can be distressing. At times, it can't be recovered either. Therefore, we recommend that you protect your important data by backing it up, i.e. copying it on a hard drive. While cloud storage is convenient and does not require any physical equipment, the data you upload on it exists online. It can be hacked into or stolen as well. But more importantly, what goes online once leaves a trace forever. So, it is better to use a hard drive or USB drive to store important personal data. However, you must always keep the hard drive in a secure spot that you will remember so that you don't have to worry about having to look for it.

Up your password game

You don't want to have a weak password that is easy to guess. It is not enough to have just a long password. Instead, you should think about strong passphrases, which are longer than the six-to-eight-character passwords and are harder to crack if created cleverly.

be 18-30 characters long.

contain more than one word.

consist of words that can't be found in dictionaries or are not famous quotes.

Your passphrase should:

consist of both uppercase and lowercase letters, numbers and symbols.

be based on personal, easy-to-guess information such as birthdays, pet names etc.

Your passphrase should not:

be based on personal likes and dislikes or hobbies.

be written down on a piece of paper or a document on your device.



TIP: Best friends and loved ones don't ask for your password. Instead, they value your privacy. Do not share your password with anyone unless there is risk to your safety and that of others.



TIP: Old is not gold, it is unsafe. Keep changing your passwords regularly.

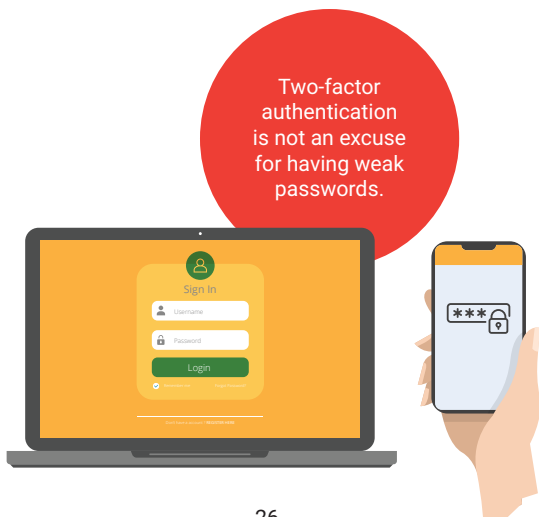


If remembering several passwords is difficult for you, Keepass has a solution. It is a free, useful tool that generates and stores strong passwords for you. You just need to remember one master password, which should be a strong, uncrackable passphrase. But make sure you store your Keepass database on external storage because hackers may be able to access it if you store it on your computer.

Two-factor authentication

Two-factor authentication is simpler than you think. You just add an extra layer of security by linking your phone and mobile phone number with your online accounts. This way, whenever you log in, you will be required to enter or select a code that will be sent to your phone via text message, an automated phone call or through an app such as Google Authenticator.

Authenticator apps are ideal for users in countries like Pakistan where mobile phone signals can be blocked on Eid or other occasions. These apps will give you a code each time you open them. They are also useful when you are travelling abroad and forget to turn off two-step verification.



Browser security

Internet Explorer, Mozilla Firefox and Google Chrome are examples of internet web browsers. Even if you are running regular anti-virus and anti-malware scans, your browser can still be vulnerable to threats. Therefore, you should ensure some additional steps for your browser's security.

1. Do not leave your accounts signed in, even if you are the only person who uses your device. You can lose your device, it can get stolen or your device could be hacked.
2. Use a private window (Firefox) or go into incognito mode (Google Chrome) so that your browser does not save a record of the websites you visit or the passwords you enter.
3. Never save your history. You can change that in your browser settings.
4. Clear your cookies and temporary internet files regularly.
5. In browser settings, enable a 'do not track' option so that websites cannot track you.
6. Never enter your password on a website that is not the official email or social media website.
7. Never give out sensitive information such as your credit card information on random websites.

Browser add-ons

You can add an extra layer of security to your browser through add-ons or extensions. They can protect your privacy and security by blocking cookies, trackers, and pop-up ads.

1. **HTTPS Everywhere:** This add-on ensures that you are connected securely to a website through HTTPS, which will keep your information private rather than an insecure one (HTTP) wherever possible.
2. **Privacy Badger:** This add-on ensures that other websites don't track you.
3. **NoScript:** A script is a little program that some websites will run in your browser. Sometimes, these scripts can have security vulnerabilities and that is why you need NoScript, so that no script can run in your browser without permission.



How to keep your social media secure and anonymous

Social media can become a headache if your security is too relaxed. This is a consideration that you have to be very careful about, especially because social media platforms are constantly changing their security and privacy settings. This means that content that was previously private or visible to only specific users can suddenly become visible to all your friends or to the public.



Basic tips for online security:

1. When making a public post, be careful about the information you share. If you do not stand on the streets to hand out your personal photos to random passers-by, there is no reason you should be doing so online. Information that can identify you should be shared online.
2. Keep checking your security and privacy settings to update them. It also helps ensure that changes made by social media platforms do not affect your security and privacy.
3. You can maintain anonymity by changing your privacy settings to prevent users from looking you up through your email address or phone number. You can also prevent users from sending you messages by controlling your privacy settings.

4. Facebook and Google allow to see where you are logged in and which browsers you are logged on to. Review this information regularly to ensure that you have not accidentally left a session logged in anywhere, or that your account has not been compromised.
5. Ensure that social media websites cannot personalise ads, or track you online. Check your Facebook ad preferences - you will be shocked to see the large number of keywords used to identify your “ad preferences”.
6. Do not let social media websites track your location. Make sure that you disable the option in your settings.
7. Never announce on social media where you are via the “check-in” option.
8. Check and control your tag settings to ensure that you are not tagged in irrelevant photos or updates.



TIP: Everything you do online stays online. Even if a website gets deleted, there will be a cache that will have your website entries available. Therefore, use social media with the knowledge that nothing is truly private in the digital sphere.

VPN

VPN stands for virtual private network. You can use a VPN to hide your location by directing your browser to servers in other countries.

Hotspot is a VPN service that you can install on your computer for free. However, it can slow down your computer. It also retains usage logs.

The best option is to look at paid but more secure VPNs such as Disconnect or Tunnelbear. Another option is to install a VPN add-on, such as Zenmate, in your browser.



ZenMate

GPS

We recommend that you do not allow your devices to access your location. While we all use location services on our phones and other devices to get directions from online maps, we often forget that in doing so we are allowing the application to access our location at all times unless we switch it off. If you don't disable location services, your devices can be easily tracked to find out where you are physically.



TIP: If you want to check direction or need to use a map, put on your location service only when you are using the map. Make sure that you keep it switched off at all other times.

Understand cyber-harassment

What would you do if someone starts knocking on your door as and when they please to yell at you, abuse you and demean you? Or that someone shouts abuses all day and night standing outside your house? You would call the police or some form of help, right?

Usually, harassment is taken seriously when it happens in physical spaces. However, people are usually ignorant towards the same when it occurs in cyberspace. We respect people's space when its physical, such as their house or office. But when someone speaks about being harassed or bullied in digital spaces, most people are quick to blame the victim.

It is important to remember that one's online space is just as valuable as one's physical space. As with any public space, the internet belongs to everyone. In physical public spaces, no one has the right to make you uncomfortable by invading your personal space, or to bully or harass you. The same principles apply to your personal space in online public space as well. Therefore, there is no reason you should put up with cyber-harassment.



Sometimes, we block people to stop them from further abusing us. But some online abusers, commonly known as trolls, keep setting up new accounts even when you block them. Have you thought about why they do this? We think they want to silence you. And it's not okay to put up with being silenced.



Remember:

- ✓ if someone is being mean to you online or saying things that distress you, it is never your fault.
- ✓ even if you're expressing an opinion that others do not like, you do not deserve to be bullied or abused.
- ✓ you are never asking for it.



Remember:

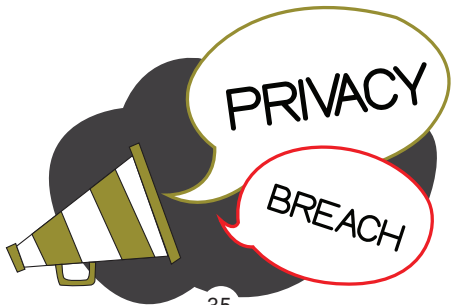
- ✓ you are online because you have a right to use the internet
- ✓ anyone who tells you to stop using the internet is asking you to give up your right
- ✓ you decide which online abuser you want to block and which to confront. Some people engage with trolls and it works sometimes.
- ✓ if you deactivate your account after being cyber-bullied, your bully has won. You have given up your space

What to do when there is a privacy breach?

If someone gains access to your computer or mobile phone and steals or exposes your data, a privacy breach has occurred. A privacy breach occurs when someone accesses information without permission.

Some steps you should take after a privacy breach:

1. Reset your password: Make sure you have different passwords for your accounts on different websites.
2. Set up two-factor authentication.
3. Monitor your banking activity and change your PIN if you see something suspicious.
4. Freeze your banking transactions if you see some suspicious activity on your account.
5. Secure your smartphone by creating a strong passcode, using a fingerprint or face scan to lock your device, etc.
6. Use good-quality anti-virus and anti-malware software.



How can your data be used against you?

Stolen data typically ends up on the Dark Web, which is the part of the Internet most people never see. Cybercriminals use it to buy and sell your personal data among other things. You make it easier for hackers and scammers when you reuse the same password across different websites. It allows cybercriminals to use your stolen login from one website to hack into your account on another. Especially if your banking details are stolen, you can also suffer financial losses. Theft of other personal data that can identify you can mean that those who have access to your data can possibly impersonate you as well. This can potentially compromise your physical safety as well.



Visit:

<https://haveibeenpwned.com/>
to see if your email address
is part of a data breach.



PARENTS



The internet can be an exciting space for children. However, it has its perils as well. Therefore, it is crucial that parents have conversations with their children about online safety as part of conversations about physical safety. Open conversations are key in supporting your child in leading a safe and positive life online. You should also encourage your child to talk about what they enjoy about going online.



If your child comes to you with a problem, be calm and curious and do not get furious.

We discourage parents from adopting a controlling approach towards children and their online presence. Your role as a parent should be more of an enabler, i.e. someone who equips their child to protect their own privacy. In Pakistan, many parents tend to adopt a very repressive and authoritarian character towards their children. While they mostly do so out of safety concerns, it is largely ineffective as they fail to forge a relationship of trust with their children. In the absence of a trust relationship, children can be more vulnerable to certain dangers as they develop sneaky behaviours and engage in things in secrecy. Banning online spaces as a method of regulation is not a viable option as it is becoming increasingly impossible given the ubiquitous nature of digital spaces. Moreover, withholding the internet is tantamount to denying opportunities for your



child. Speak to children the same way you do about the physical world, information shared online has similar repercussions as the real world. Use examples from the real world to draw analogies with virtual spaces. For instance, sharing ones pictures on a public platform is akin to making photocopies and distributing them at a public crossing. However the final decision making should be left up to the child.

You should particularly talk to your child about how predators may pose as a child or teen on social media websites. By doing so, they then can encourage the child to exchange personal information.

Adopt a non-judgmental approach when your child talks about a challenge online. Thank them for telling you about it. Instead of a pinning-the-blame approach, adopt a problem-solving approach. This will not only strengthen your trust bond with your child, but will also enable them to learn problem-solving methods by seeing you set an example.

Here are some tips that you could use while speaking to your child about online safety:

- Speak to your children about appropriate online behaviour and online safety at an early age.
- Encourage them to talk to you when they feel uncomfortable and take them seriously when they report to you about something unusual.
- Talk to children about boundaries online, speaking to strangers.
- Talk to children about the importance of making strong passwords and never sharing them with others.
- Talk to children about viruses and the need to scan their devices.
- Talk to children about the need to protect their personal data and the importance of not sharing it with strangers.
- Talk to children about how strangers do not always tell the truth and therefore must not be trusted.
- Go through privacy settings with your child with the approach of enabling your child to think about it on their own.

- Explain to your children that these measures are not meant to curtail their activity. Instead, they are aimed at protecting them from some people's potential behaviour.
- Set ground rules for your child's usage of social media such as number of hours allowed, appropriate time of the day, etc. But try to do so by taking them on board in developing these rules instead of adopting a top-down approach of imposing rules from above. Also, make some rules for parents, too, and abide by them to set an example.
- Give them incentives for encouragement for, say, running malware scans. Incentives could be extra time to use the internet.
- Don't be a spy - make your children understand social networking etiquette instead of always "keeping an eye". It will build a trust relationship and your kids will approach you when something odd occurs.



TIP: Teach your kids not to yap about their YAPPY with strangers.



Protect your child's privacy on your own social media

Nowadays, a number of social media users put up photos and other details about their child - sometimes, even before the child is born! Creating a digital footprint of your child even before they are born by setting up social media accounts in their name may have consequences. It does not grant the future child the agency to consent. Similarly, infants cannot give or deny consent regarding use of their photos on their parents' social media.



TIP: Blur out pictures of your kids if they cannot give or deny consent. Similarly, make it a point to say no to your relatives and friends when they try to photograph your child.



Privacy does not mean secrecy

Do you tell strangers on the street your secrets and share your personal information? If no, then there is no reason you should be doing so online.

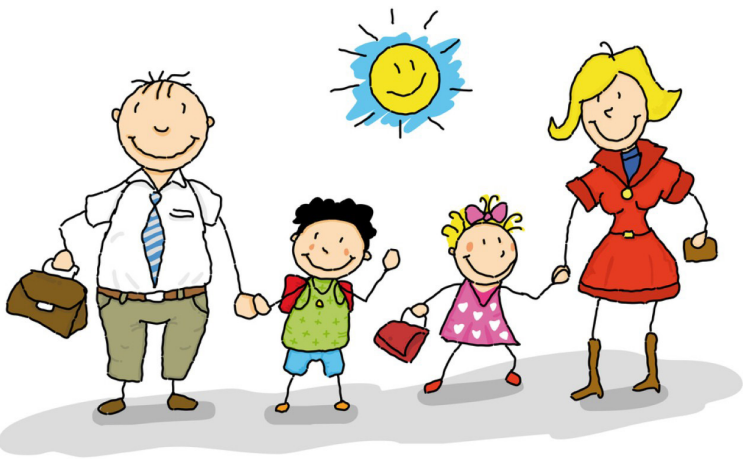
Privacy should not be conflated with secrecy. You are not being secretive if you lock the doors of your home at night. You are simply taking care of your privacy. The same rule applies to online spaces. Your control over what you share and what you don't share with the online world is not the same as being secretive. It simply means that you are taking control of your privacy.



Set a good example

Children and young adults are extremely intuitive and tend to pick up behaviours of those around them. Role models are an important tool for instilling healthy habits among children. For instance, if your child sees you posting family pictures without any regard for privacy they are less likely to care about privacy themselves. Practice what you preach!

Ask your children before posting content about them, be it a vacation picture or their exam report card.



Resources

<https://www.childnet.com/resources>

<https://www.saferinternet.org.uk/advice-centre/parents-and-carers>

<https://www.esafety.gov.au/parents>

<https://www.common sense media.org/>

<https://bullyingnoway.gov.au/RespondingToBullying/GetHelpandMoreInformation/Pages/Online-safety.aspx>

<https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/talking-your-child-staying-safe-online/>



Digital**Rights**Foundation
"KNOW YOUR RIGHTS"

Supported by



**FRIEDRICH NAUMANN
FOUNDATION** For Freedom.

Pakistan