Parents' Guide to Protecting Children's Privacy and Personal Data on the Internet

Дирекција за заштита на личните податоци

METAMORPHOSIS
Foundation for Internet and Society

Skopje, June 2015

The parents' Guide is developed within the joint cooperation between the Directorate for Personal Data Protection and the Metamorphosis Foundation for Internet and Society and secondary schools in the city of Skopje, as a part of the project PRIVACY LESSONS

The Guide was authored by:

- **M.A. Ljiljana Pecova Ilieska, Directorate for Personal Data Protection**
- **M.A. Tamara Resavska, Metamorphosis Foundation for Internet and Society**

Дирекција за
заштита на
личните податоци

Contact:

Directorate for Personal Data Protection

Bull. „Goce Delcev" No.18 1000 Skopje, Macedonia

Tel: ++ 389 (0) 23230 635

Fax: ++389 (0) 23230 635

Email: info@privacy.mk

Web: www.privacy.mk

METAMORPHOSIS
Foundation for Internet and Society

Contact:

Metamorphosis, Foundation for Internet and Society

St. „Apostol Guslarot" 40

Skopje, Macedonia

Tel: ++ 389 (0) 23109 325

Email: info@metamorphosis.org.mk

Web: www.metamorphosis.org.mk

Introduction

While some things change over the years, other remain the same. Children have the same need for communication, the need for socialization, to have fun, but besides that it is more than necessary to protect their privacy by preventing the abuse of personal data.

This Guide does not aim to upset you, as parents, and to create fear for the new world of technology used by your child, yet simply to contribute to raising awareness of the operation of new technologies, how you can jointly explore through "a sea of information" with your youngsters, how to protect your child from accessing inappropriate content and communications, as well as what are the mechanisms for reporting, if you or your child, encounters a misuse of personal data on social networks.

The focus of this Guide lies on the Internet, on social networks, and also presents other forms of communications and key locations where misuse of personal data and invasion of privacy is possible.

Showing interest in the technologies used by your child, you can learn together with him/her and know what he/she is actually doing when "sitting on the internet."

The authors

About the Guide

This Guide emerged as a need, taking into account the analyzes made by the Directorate for Protection of Personal Data in 2014, as well as the research conducted within the project PRIVACY LESSONS in 2015, where following results were observed:

- 64% of parents believe that their children are not familiar with privacy policies regarding the social networks they visit

- 68% of the parents are most frightened by social networks, and believe that they are the biggest threat

- 60% of the parents believe that, as parents, they have more important role in the education

All this was an indicator for us, that is more than necessary to start working on a Guide that would elaborate the topics of privacy protection, personal data protection and children's online safety as well as all possible challenges posed by using the Internet itself. We are confident that we are going to make this information more relatable to each parent in this manner, and that we will act preventively by raising public awareness of personal data protection when using social networks. At the same time, we hope that it will serve as a guide with useful recommendations, while promoting reporting mechanisms available to the citizens.

Dimitar Gjeorgjievski

Director, Directorate for Protection of Personal Data

With the ever-increasing daily usage of the Internet and social media, parents are faced with new challenge, which is how to protect their children from the risks that are posed by the Internet and also to learn to use it safely and responsibly. The Foundation "Metamorphosis" with its long work in this field has developed multiple resources intended to educate children and parents on how to protect their privacy and how to safely and securely use the Internet. This Guide is an extension of these efforts and contributes to raising awareness among parents about privacy protection. Our goal is not to scare parents from the Internet and new technologies, but quite the contrary, to provide maximum benefit from the Internet by being up to date with changes in the digital world, to gain new skills, to encourage thinking about issues related to the risks and benefits of using the Internet, and also we will help them to cope with the challenges they face in educating children about safe and responsible usage of the Internet.

Bardhyl Jashari,

Director, Foundation Metamorphosis

Contents

Chapter 1

What is Internet?

Internet is a set of worldwide distributed computers connected to each other for information exchange. The term is a combination of the words "**Inter**national and "**net**work".

“The Internet was originally conceived as a huge database for use in scientific and educational goals. Hence, the main role of the Internet was archiving and communicating. As the number of computers connected to the Internet was growing, so did the number of organizations offering online information and the number of visitors to websites (which are potential users of products and services).

Today, the Internet provides multiple services:

1. **Information** via:

-World Wide Web (Cobweb widespread worldwide) (WWW) - comparable with consulting the digital library
-News groups - comparable with magazines on various topics

2. **Communication** via:

-Sending and receiving emails:
-Program conversation: through direct connection similar to a telephone conversation, allowed through a program that provides real-time chat
-Electronic mail (email): through indirect connection, similar to mail
-Discussion groups: through messaging within a group (discussion groups, news groups)
-Conference: through direct and simultaneous connection between multiple users
-Data transfer:
-FTP service (file transfer protocol), which enables quick file exchange
-Attaching files to messages sent by email
-downloading from the internet via WWW
-from point to point, which allows copying files from other PCs free or at a certain favorable price.[1]

Glossary of terms related to the Internet

[1] 1 "Manual for Information and Communication Technology" - 2006, USAID e-Government Project, Link: http://aa.mk/WBStorage/Files/Priracnik%20IKT%20Mak.pdf

1. **What is a social network**?

a. Online community of people with common interests who use webpage or other technology in order to intercommunicate and share information, resources, etc.

b. Website or online service that enables communication.

2. When your child goes "**online**" it means that he/she connects to the Internet. Although WWW is only part of the Internet, however terms such as: **Web**, **Internet** and **Net**, often are used to indicate the same - connecting to the global network of information and communication.

3. The **Web** also means a set of several **Websites** on the Internet. It contains knowledge and information for every possible subject or object of interest. Website is a www. page which contains information. For instance, the website of the Directorate for Personal Data Protection is www.dzlp.mk. This is the **web address** of this institution.

4. **Social networking** is the use of websites or other online technologies in order to communicate and share information, etc.

A recent research showed the top ten most popular networking social websites :

Facebook 900,000,000 - monthly visitors
Twitter 310,000,000 - monthly visitors
LinkedIn 255,000,000 monthly visitors
Pinterest 250,000,000 - monthly visitors
Google Plus + 120,000,000 monthly visitors
Tumblr 110,000,000 - monthly visitors
Instagram 100,000,000 monthly visitors
VK 80,000,000 monthly visitors
Flickr 65,000,000 monthly visitors
Vine 42,000,000 - monthly visitors
Meetup 40,000,000 - monthly visitors
Tagged 38,000,000 - monthly visitors
Ask.fm 37,000,000 - monthly visitors
MeetMe 15,500,000 - monthly visitors
ClassMates 15,000,000 - monthly visitors

Communication on social media often contains abbreviations, which are only recognized by young people. Thus, you can find a list of frequently used acronyms by teenagers on the internet (Appendix 1) which are deciphered particularly for confused parents.

Social Media Privacy Policies

Privacy policies are rules that inform all of us as Internet users how and why the data are collected. If we want to know how to manage information and how we can protect our online privacy, we should carefully read and continually follow these privacy policies, because they are a subject to change.

For instance, many of the services require you to create a Google account. In order to do so, you need to type your personal information such as: name, surname, e-mail, phone number or credit card to store your profile and so forth. If you want to fully use the offered options for content sharing, you are required to create a public profile on Google or make the existing one public, which includes public display of your name, surname and a photograph.

Additionally, websites collect data only by using their services. Namely, they collect data about the device, e.g. your hardware model, version of the operating system, mobile network information, which includes your phone number.

In particular, when you use Google services, your location data, IP address, Wi-Fi access point, etc. can be collected and processed. Also, identification data for your browser or device can be collected by using Cookies.

Cookies are small text data files which can be saved on your hard drive by some of the websites you visit and are usually used for advertising purposes, but they also follow ("hunt") your movement (while surfing) on the website[2].

[2] http://www.google.com/policies/privacy/

Always, seriously, always!, read the social media privacy policies and services they offers because therein lies the answer on how to protect yourself if your child's privacy is violated[3].

[3] https://www.facebook.com/about/privacy/

Chapter 2

What is privacy? Which are the personal data that reveal our identity?

The right to personal data protection and the right to privacy are two different human rights. Due to the great importance of individual's privacy, in most countries throughout the world, this right is regulated by the Constitution as the highest constitutive act of the state, as is the case with Republic of Macedonia.

In our Constitution, the section dedicated to Civil and political rights and freedoms, covers several human rights that are components of the right to privacy, since privacy is a broad, complex concept that summarizes several individual rights. In this regard, it is important to mention the following rights:

- Every citizen is guaranteed the respect and protection of privacy of its personal and family life, of its dignity and reputation (Article 25).
- Every citizen is guaranteed the inviolability of the home. The right to inviolability of the home may be restricted only by court decision when related to crime detection or prevention or health protection (Article 26).
- The freedom and confidentiality of correspondence and all other forms of communication are guaranteed. This right may be waived only on the basis of a court decision and in an appropriate legal procedure (Article 17).

The rise of the privacy right to a rank of constitutionally guaranteed human right, indicates the great importance of this right for the individual, who carries certain rights/authorizations and duties/responsibilities too. Not only this right applies to the individual right-holders, but also applies to other individuals, and the state and its institutions as well. These are the three Articles in the Constitution that guarantee privacy. The Law on Personal Data Protection applies only to the rights of the citizen to protect his/hers personal data.

There is no specific Law on Privacy Protection in Macedonia, whereas in the US, there is the special Children's Online Privacy Protection Act[4] and it refers to the online collection of personal data by legal or physical entity under US jurisdiction from children under 13 years of age. This means that the information that must be included in a privacy policy by the website operator are defined, when and how to seek consent from a parent or guardian, and which are the operator's responsibilities in order to protect children's privacy and internet safety, including marketing restrictions for youngsters under 13 years of age.

Personal data that reveal our identity are:

- Name and surname

- Primary place of residence

[4] https://en.wikipedia.org/wiki/Children%27s_Online_Privacy_Protection_Act

- Identification number
- Gender etc. i.e. anything that could lead to identification and verification of a person's identity.

What are the dangers that lurk children on the Internet?

With the development of new technologies and means of communication, our biggest concerns are that children will come in contact with the wrong people when online, that they will have access to inappropriate content or materials and that they might get abused in any way.

Here are some of the most common risks to your children when online and misuse of personal data that you may face, as well as recommendations how to deal with them.

Identity theft

Identity theft is a form of stealing the personal identification data of some other person whereby the thief pretends to be someone else, taking the identity of the another person, usually in order to access that person's resources or to obtain funds and other benefits on behalf of that person.

Identity theft is often used as a method to carry out criminal activities and includes unauthorized use of your personal information, usually including bank data that can be used to defraud you or to commit crimes on your behalf. Identity theft can be committed online, can be committed by using physically printed documents, or as a combination of both.

Child Identity theft occurs when personal data and personal identification number of a minor is being used by another person for personal gain, usually financial. The intruder may be a family member, friend or even a stranger.

Some of the ways for committing identity theft:

- Personal data theft from computers by using malware, especially Trojan horse or other forms of spyware
- Guessing the Unique Master Citizen Number digits by using information found on social networks such as Facebook (e.g. publicly presented dates of birth)
- Publicly shared photos that can easily be downloaded from websites
- Befriending strangers on social networks and taking advantage of their trust to get to personal data.

Therefore, advise your children:

- Not to share personal data with their friends, acquaintances and other people.
- Always to have effective and updated antivirus and anti-spyware on the device they use for accessing the Internet.

- Never to give out personal information as a response to an e-mail, letter or phone call if they are not sure that the application is from a secure source.
- To inform you immediately if they have received a suspicious e-mail that contains a request for disclosure of any kind of personal data.

What is phishing?

Phishing is a form of fraud that covers a set of activities of unauthorized senders, by using fake email messages and fake websites of many financial organizations, trying to obtain users' confidential personal data such as UMCN, username, PIN numbers etc. Unfortunately, a large number of users are not familiar with this type of fraud. Once they get the confidential data, the malicious senders either use them on their own or they sell them. The messages usually refer to fake websites, which look completely the same with the websites of the legitimate companies (firms).

Most frequent phishing forms are:

- Fake bank alert or alert from other financial institution in which the user is required to state personal data to prevent suspending/closing the account.

- Fraud by bidding websites, which convinces the user to pay a certain amount of money to buy a certain product and with that to make the user think that he/she's buying some kind of product, whilst he/she actually performs payment to a false account.

- A fake message from the administrator in which data is requested by the user, such as password.

- Various announcements which try to extort money for bogus charities.

- Messages that entices the user to pay a certain amount of money to a false account (for example, a message for a drastic discount of a product that can be bought only on the Internet).

- Messages that inform you that you have won the lottery and they need your personal data so you could be able to claim the prize.

How to recognize phishing message?

Fraudsters often copy the visual appearance of the actual webpages of banks and other companies. Lately, the false messages are completely identical to the originals, but still, there are certain details that may reveal the fraud:

- Spelling and grammar errors;
- They require personal data;
- They require installing a program that claims to repair the discovered safety oversight;
- Fake links and messages;
- Not using SSL and digital certificates;
- The content of the message's in HTML form;
- Unrealistic promises;
- Errors in the message’s subject line;
- They require an immediate response;
- Doesn’t refer to a particular person;

Hate speech

Hate speech is biased, hostile, malicious speech addressed to a single person or a group of people because of some characteristics they have, or because of the assigned characteristics[5]. In the broadest sense, hate speech is used in all forms of expressions that spread, spur, promote or justify hatred based on intolerance on any other form of discrimination.

Hate speech is an abuse of freedom of expression which includes the violation of the rights of others.

Online hate speech ("cyber hate") means any use of the electronic communications technology to spread anti-Semitic, racist, xenophobic, discriminatory, extremist or terrorist content.

The term *online hate speech* is broader than the term *Internet hate speech*, because besides the Internet content (webpages, social networks, user-generated content, blogs, online games, e-mails etc.) it also covers cell phone content too.

How does hate speech look like?

Through the prism of humor, French Twitter users post messages of hate towards Jews grouped under the hashtag "#unbonjuif", "#unjuifmort"(“#goodjew”, “#deadjew”).

French associations filed a lawsuit against the company because of Twitter public spurring of discrimination, hatred or violence. After the lawsuit, the company was obliged to give information that can identify Internet users who were authors of the tweets.

What to do if your child is a victim of online hate speech?

[5] Based on one or more characteristics specified to their physical, psychological, mental, economic, cultural or social identity.

- Report the crime to the police or Public Prosecution. According to the Criminal Code of Republic of Macedonia, spreading hatred is a crime which follows a sentence of 1 to 10 years in prison. It can be reported anonymously in MIA, in the nearest police station, by dialing 192 or by sending an e-mail to the Department of Cybercrime at cybercrime@moi.gov.mk.
- On the Facebook and Twitter social networks:
- Reply to posts or tweets that spread hatred, pointing out to the author what he/she is actually doing, as well as using the hashtag #donothate or #mosurrej.
- Use the mechanisms for ready-made report button offered by the medium through which the message is being communicated.

Remember: Hate speech thrives the most when nobody opposes. Because bullies are often cowards, they often withdraw at the first sign of resistance. You can read on the subject related to reporting hate speech in the section "Guidelines" on the website "Do not hate" (nemrazi.mk/category/upatstva).

What is cyberbullying?

The social fellowship and the many possibilities offered by the Internet are the hallmark of the 21st century. Children's lives take place in several places at once, not only at school halls, or their friends' homes, but on the internet as well.

Most children and teens spend a great deal of their time on their mobile phone or computer, chatting with their friends, posting photos, videos and music on different social networks that allow socializing and entertainment. They might have online friends who they've never met in person, friends with whom they play games and exchange messages.

Online-violence, called cyberbullying, occurs when children and teenagers using the Internet, mobile phones or other technological devices, publish insulting information in the form of texts, images or other content, intended to hurt or embarrass another person.

How does cyberbullying look like?

- Harassment - constantly sending offensive, disturbing and harsh messages and pornographic materials.
- Imitation – hacking into other users' accounts and sending false, embarrassing messages on behalf of the hacked user.
- Derogation - writing rumors or other false statements that can harm the victim, as well as sending and posting online images with humiliating content and embarrassing personal information.
- Defrauding and public disclosure - sharing someone else's personal information or deceiving someone to share his secrets in order to forward them to others
- Vulgar speech - sending messages with vulgar content
- Cyberstalking - constant intimidation of the victim for his/hers safety

What if your child is a victim of cyberbullying?

- Advise your children to block communication with the cyberbullies, not to open and not to respond to e-mails or messages from someone who they know is a cyberbully.
- Ask them to show you the messages and together discuss their content.
- Keep or print all the messages sent from the bullies as evidence that latter on you can show to the web service providers, or even the police, who could deal with the bully accordingly.
- If your child's personal data is being abused on the Internet, you can report the case to the Directorate for Personal Data Protection (www.dzlp.mk).
- For severe cases of cyberbullying, which include physical violence threats, you can go to the police.
- Please report abuses to the websites and social networks that have adequate options aimed at blocking a particular person or message (Report or Block) or report inappropriate content, or directly address the administrator.
- Most importantly, talk to your children about what they do online.

Online predators

The Internet is more anonymous than the real world. People can hide their identity and even pretend to be someone else. This can pose a real danger to the children and teenagers that are online. Online predators may try to lure children and teenagers into sexual conversations and even personal meetings. Predators can sometimes send inappropriate content or ask children to send photos. Therefore, it is important to teach your children always to be careful when online.

Online predators are generally greater risk to teenagers because they are curious and want to be accepted, they could voluntarily talk to a predator, even if they know that it's dangerous. Sometimes they may believe that they are in love with someone online, increasing the chances to agree to meet in person.

How can you know if your child might be a victim of online predators?

- If your child is enticed by a predator he/she can spend a lot of time in chat rooms.

- Your child receives phone calls from people he/she never met before or calls numbers you do not know.

- Your child receives gifts in the mail from other cities or abroad by people you do not know.

!Predators often send letters or gifts to their potential victims.

What kind of advice should you give to your children:

- To avoid suggestive names or photos that could attract predators' attention. Eg. Sexygirl15, hotboy2001.

- If someone is flattering them and giving them compliments online they should be very careful. Predators may use flattery compliments in order to try to start relationship with teenagers. This does not mean they have to question everything, but should be careful.

- Not to talk to anyone who wants to talk about personal matters too. If someone wants to discuss things that are sexual or personal, the conversation should be ended.
- They need to have in mind that people are not always as they present themselves. Predators can pretend to be children or teenagers in order to talk to children online, they can use a fake photo or add other information to their profiles to look more convincing.
- Never to agree to meet someone they have met online. Predators may try to arrange a meeting with a child or teenager. Even if a person looks polite and harmless, this can be very risky.
- They should immediately tell a parent or an adult they trust when facing a problem. If someone made them feel uncomfortable online, they should tell their parents or an adult they trust. At the same time, they need to preserve e-mail messages and other communications with the predator, as it may be needed as evidence.

Remember:

- Talk to your children about online predators and Internet dangers.
- Place the computer in a common room where you have a view and you can monitor your child while on the Internet.
- Set a time limit for using the computer.

Video games addiction

Video games addiction is an excessive use of computer and video games, which affects the person's everyday life.

Some of the emotional signs of video games addiction are the sense of restlessness or anxiety when not playing, preoccupation with thoughts of the previous online activities or anticipation of the next session, lying to friends or family members about the time spent playing games, isolation from others to spend more time in playing.

Signs which can help you recognize video game addiction:

- Preoccupation - The child spends a lot of time thinking about games, even when not playing or plans what to play next.
- Withdrawal - Feeling of restlessness, irritability, moodiness, anxiety or sadness when the child tries to reduce the time spent on playing or stop the game or when he/she can't play at all.
- Tolerance - The child feels that he/she must play more and more, he/she must play more exciting games or use more powerful equipment to achieve the level of excitement as before.

- Reduction/termination - The child feels that it should play less, but cannot reduce or shorten the time spent on playing games.
- Quitting other activities - The child loses interest or participates less in other recreational activities (hobbies, meetings with friends) because of video games.
- Continues despite the problems – The child continues to play video games although aware of the negative consequences, such as lack of sleep, being late for school, spending money, arguing with others or neglecting important tasks
- Fraud/cover – The child lies to the family, friends and others about the time spent playing video games.

What to do if your child spends too much time playing video games?

- Limit the time your child spends on the computer.
- Talk with your child about the negative sides of excessive gaming and lack of socialization
- Watch the latest blockbuster at the cinema, make a chore for your child inflate his bicycle tires, encourage your child to go out and have fun with friends.
- Remind them that there is life outside of video games - do not forget to live it.

What do professors say about the subject?

What challenges faces a student who has a social networks profile?

We asked for answers from several project coordinators of the PRIVACY LESSONS project:

M.A. Nikolina Ivanovska, psychology professor in the secondary school "Nikola Karev"

“A minor student that has a social network profile can encounter both advantages and disadvantages. Parallel to the already known advantages in terms of socialization, instant access to news and information, etc., there are certain disadvantages that are often unconsciously overlooked, and represent certain deficiencies and have a major influence on the development minors’ personality. Oftentimes, we encounter cases where the self-valuation is based on the number of likes on a photography, and that directly affects the more serious segments of personality development due to the gap between the ideal and the real self-image and the likelihood of psychological disorders that the minor can face.

Labeling, hate speech, mass dissemination of any position by a particular group, also have a huge impact on the development of personality, and this influence, unfortunately, is overlooked by the adults. As teachers and parents, we do not always pay enough attention to the dangers hidden under certain titles, persons behind some accounts and the huge number of fake profiles that our children are in contact with, etc.

The presence of collective attitude of adults, who do not take social networks seriously and the impact social networks have on the children can be largely felt, and this puts the whole educational process of the children into question.

As educators and parents, we are obliged to keep up with the modernization of technology and the development of social networks that are the engine of modern society and understanding and following the principles of these networks is the only way to influence the development of our children, and by doing so, we can create persons that will successfully detect and avoid dangers they are exposed to."

Anita Armaginijan- Tasevska, school teacher in high school "Arseni Jovkov" says:

"Modern society brings changes that we can all feel as parents, teachers, and even our children can feel them. These changes are visible around the 12th to 15th year of age, and the children feel the need to be active on social networks.

Are we as parents, teachers and professionals ready to explain to our children what is most important, are we ready to devote time to the children, are we ready to see what they post on social networks as an indicator of the changes they experience? Social networks offer a variety of information, images, representations of something new, interesting, but the question is: have the children or students figured all this out and can they utilize it?

The parents' opinion usually goes from one extreme to the other, from allowing children to do everything to restrictions and prohibitions. We mustn't forget that children come to school with expensive mobile phones and tablets, wanting to show their status, but also often using their devices during lectures, wanting to have all the information and messages that are transferred to the social networks.

As a parent, teacher and associate I believe we should leave the childhood to the children to experience it when they are still children, to play with toys and with their friends, because that period of their life can never be rewritten.

My opinion is that in this period, the children or the school students are ready to share information with their peers, but it all depends on children's maturity and responsibility, on one hand and unsuspecting control of the parent on the other hand."

What do the parents say?

What is the attitude of parents to posting photographs of children on social networks?

Suzana Avramovska, parent of a secondary school student from the Secondary School "Pance Karagjozov" says: "I am not against sharing of photos of children on social networks, if the content of these photos is not vulgar and/or jeopardizes the child's identity, on a profile protected from persons not in the friends list... Moreover, children should not have their personal social network profile, at least not until they are 15 years old... and when it comes to children older than 15, to my thinking, they should be supervised by a parent. The most important thing about social networks is not to allow children to substitute real life with the virtual one."

Parent of secondary school student from the secondary school "Josip Broz Tito" (anonymous) believes that: "Posting photographs of the child and his/hers classmates is not a problem, as long as he/she does not post inappropriate content or material that could, with the posting, offend someone or calls on hate speech. What frightens me the most as a parent is if my child is being brought into unwanted situations or drawn into conversations with inappropriate content. I consider that talking to the child would help the most in such situations, although I'm not against him to investigate certain issues on the Internet on his own. However, I avoid sharing photographs of him because my list of friends is not the same as the list of his peers. Thus, I believe that I am excluding any potential opportunities for abuse, but if he is not responsible of his own actions we can’t do anything."

Chapter 3

Reporting mechanisms

THE DIRECTORATE FOR PERSONAL DATA PROTECTION - Procedure for filing initiative for inspection - The citizens submit requests[6] and complaints[7] regarding the abuse of social networks to the Directorate. Then, the Directorate responds to the requests and complaints that refer to the most common types of abuse on social networks such as requests to delete fake Facebook profiles, or to delete hacked accounts. The Directorate also responds to the complains for detecting IP address that are later resent to the Ministry of Interior, then to unauthorized publication of photographs, complaints regarding abuse of minors' data and others. Each year the number of requests and complaints that citizens are refering to the Directorate is increasing[8].

If you encounter misuse of your personal information or the personal data of your child or you suspect child abuse, you can report to the Directorate for Protection Data Protection info@privacy.mk or dial: 02 / 3230-635

The complaint is processed immediately, reviewed and submitted to the person in charge of it. If the complaint refers to the abuse of personal data on social networks and the client requires deleting of created fake profile or hacked profile, after the reception, DPDP (including delivery of required documentation) is establishing communication with the administrative team of the respective social network for professional help about deletion through authorized persons. After the response is set, the complainant is informed immediately .

If the Directorate does not have competencies regarding the issue, the complaint shall be submitted to the competent institution and the applicant will be informed. If the complaint is submitted to several authorities at the same time, the authorities cooperate with each other.

If the complaint is unclear or cannot be responded to, it is necessary to ask the complainant to further specify it or provide evidence. Also, the applicant may be asked to elaborate on the complaint, including to be called in DPDP for further establishing of the facts. The Directorate reports on the measures taken after the complaint in any case.

If the complaint response opens a doubt for treatment of other departments within the Directorate (e.g. inspection) or institutions outside of the Directorate (e.g. Public Prosecutor, Ministry of Internal

[6] http://www.dzlp.mk/mk/prizlnlp

[7] Under the petition or proposal, the meaning of the handling of complaints and suggestions, means any written or oral speech of applicants to the bodies which act on the complaints or suggestions for protection and realization of their rights and interests, public interests determined by law or due to launch an initiative in the public interest.

[8] See Annual Report of the Directorate for 2013 and 2014,
http://www.dzlp.mk/sites/default/files/u4/Godisen_izvestaj_DZLP_2013.pdf
http://dzlp.mk/sites/default/files/u1002/MK.pdf

Affairs, etc.) persons responsible for handling complaints need to submit an initiative/request/ information to the appropriate official in the Directorate.

SCHOOL PERSONAL DATA PROTECTION OFFICER – if your child faces personal data abuse in school, you can also inform the School Personal Data Protection Officer in the school which the child attends. According to Article 26 from the Law on Personal Data Protection, each school and each controller has a legal obligation to appoint a School Personal Data Protection Officer who participates in the decision-making processes related to personal data processing and the exercise of the rights of personal data subjects. Also, he/she monitors the compliance with the law and regulations based on the law, which means he/she has an obligation to be familiar with a particular situation and to react, if necessary, by changing certain regulations and procedures at the school, unless the school does not provide confidentiality measures and personal data protection. The officer is also a key part in the process of informing the students about personal data protection, but the teachers/employees in the school as well.

Chapter 4

Useful software and accessories to protect the privacy of your children.

The software for parental control is a great way of controlling, limiting and monitoring the children's activities while online. However, their safety is not the only thing that can be questioned as a result of inappropriate use of the Internet. The safety of the whole family, as well as the computer you are all using, could also be threatened. Therefore, you should talk to your kids and give them useful tips, as well as teach them how to take care of your computer to ensure that it functions properly. Here are some useful softwares that can help you take care of your child's safety while using the internet:

- **Crawler Parental Control** is one of the few free, comprehensive and fully functional softwares for parental control. Immediately after installing, administrator password is given to the parent which allows to make the desired settings for each computer user separately. The software allows control of the time that the user spends online, and to limit the time that he/she can actually spend on the computer. Also, there is an option to restrict certain websites which you do not want to be visited by the user, websites that will be available for use, as well as an option to restrict particular words which can lead to unwanted websites.

Crawler Parental Control allows you to restric the access of specific users to certain folders or entire disks on the computer. This limitation can be complete or to be applied to certain periods of the week or the day, and there is the option of fixing the number of hours that users are allowed to spend monthly, weekly and daily as well. Of course certain programs can be blocked as well as to block access to certain system locations in order to prevent systemic changes that could disable the correct functioning of the system.

For all this, you as a parent, can receive reports.

Download link: http://download.cnet.com/Crawler-Parental-Control/3000-27064_4-10549693.html

- **Glubble** is a very popular family tool which is used as an add-on for the web browser Mozilla Firefox. Although its use is limited only to this browser, it can be used on all operating systems. With the help of this add-on the browser is divided into two parts, one is used and administered by the parents, while the second is intended for the children. A separate account can be created for each child, which will enable Internet activities adapted to his age.

At the beginning the parents set an administrative password, thanks to which they can make the desired settings, and use the browser as they need. When the child is about to use a browser, he/she just needs to choose their profile and they will get a brand new environment through which they can surf through a default list of educational and entertainment websites, they can request to visit new websites, particularly interesting sites that are just one click away from placing them in the favorites folder or to leave messages to other family members. The search possibilities are limited to safe terms only. The previously selected content that are already part of Glubble are all in English, but you can also add the Macedonian ones.

Download link: https://addons.mozilla.org/EN-us/firefox/addon/glubble-fox-family/

- **K9 Web Protection** is a free tool for filtering web content and establishing parental control over the child's activities while online. The software requires a free license to use it, and you will receive it via email if you pass the registration procedure.

What can you customize with K9 Web Protection?

With this small piece of software, in particular, you can specify the desired level of protection on the user's profile system and any violation will be disabled by a password. You can choose among the several given levels of protection, which include a restricted access to specific content types or list of prohibited content that you can adjust yourself. Furthermore, you can set the periods of the day in which the use of the browser is restricted as well as periods in which the use is allowed.

There is also the possibility to deny access to certain websites, while access others can be always granted. The access restriction can be established on the basis of certain keywords, and also there are the options for reporting and punishing if an attempt to access any of the restricted content is made.

Probably one of the most important things that this software enables is detailed system reporting, through which you can get a completely clear image of your child's online activities.

Download link :http://www1.k9webprotection.com/

- **WebFilter Pro** is a browser plugin that provides a simple way to block adult content, proxy servers and different websites for social networking without imposing time constraints or other unwanted sanctions. Users can block everything, from nudity to betting and games. This plugin provides configuration of individual white and black lists allowing access to certain websites that don't fall into any of the many filtering categories this plugin offers.

Download link: https://chrome.google.com/webstore/detail/webfilter-pro-the-best-fi/ejgfoklefkbjadjcgjmnhfbdfjolojnn?hl=en

- **FoxFilter** is a plugin designed to enable blocking filters for the users based on individual keywords and websites (eg. Playboy, nudity, curse words) offering the possibility of adding reliable websites into moderated list of content. This plugin's settings enable website scanning such as the title and URL, and users can adapt the information and warnings about the type of content based on each blocked site.

Download link: https://addons.mozilla.org/en-us/firefox/addon/foxfilter/

- **Nanny for Google Chrome, LeechBlock за Firefox** - As children grow, it seems some concerns disappear. But time management becomes a greater source of care especially for teens whose lives are increasingly starting to revolve around social interactions, or social networking sites. These extensions block specific sites at specific times of the day in order to prevent distractions and improve productivity. For example, you can block Facebook from noon to 6 pm.

These two extensions also enable you to predetermine how much time can your children spend on certain web sites in a day, which means you can allocate and hour or two on a website, rather than to entirely block access to it.

Download link :
https://chrome.google.com/webstore/detail/webnanny/pbdfeeacmbjblfbnkgknimpgdikjhpha?hl=en
and
https://addons.mozilla.org/en-us/firefox/addon/leechblock/

- **TinyFilter** is a very simple Google Chrome extension that blocks access to specific Web content based on a set of keywords that forbid access to any website that contains words from the blacklist. This extension can block web sites based on a desired URL, but the primary role is to filter content based on set keyword.

Download link :
https://chrome.google.com/webstore/detail/tinyfilter-reliable-conte/nlfgnnlnfbpcammlnibfkplpnbbbdeli?hl=en

- **Golden eye** it is a powerful software for spying and monitoring of all computer activities: entering passwords and other data, visited websites, used applications and all that verified with images captured at the moment of use. This software costs $29.95.

Download link: http://www.monitoring-spy-software.com/

- **Safe eyes** encapsulates all the options necessary for parental control: restricts access to certain types of web sites and programs, limits the time for various activities on the Internet, keeps notes of the activities and gives report on violations in several ways. The license for the software costs $49.95.

Download link: http://www.internetsafety.com/

- **Web Watcher** is one of the best software for Internet-filtering, blocking programs, time limitations and advanced monitoring of the child's activities while he/she uses the computer. License cost is $97.00.

Download link: http://webwatcher.com/

- **Cyber Patrol** is a parental control program with a wide array of options for filtering, blocking programs, time managing and monitoring, and is designed for advanced users. This program has 14 days free trial period, and the it costs $39.95 annually.

Download link: http://www.cyberpatrol.com/

- **Net Nanny** is a parental control software with filtering features, opportunities for blocking chat-apps and file sharing programs, groups (newsgroups) and with weaker opportunities for monitoring the activities. You can test it 15 days for free, and usage has a price of $39.99 per year.

Download link: http://www.netnanny.com/

- **Parental control** bar allows filtering of undesirable web contents and offers easy switching from parental mode which is password protected, to children's mode.

Download link: http://www.parentalcontrolbar.org/

- **KidZui** is a browser for children from 3 to 12 years of age. It allows the children to experience multimedia internet-content, while allowing parental control.

Download link: http://www.kidzui.com/

Tips on how to protect your children’s privacy

Set some ground rules - Children need to know under which conditions, in which periods of the day and how they may use the Internet. These conditions need to be specified by you. Begin with, for example, by allowing your children to go online only after they have completed their school obligations.

Computer on a visible spot - Place the computer in a central place in the room or in the classroom so you can monitor them from time to time. This is important so you can see if your kids accidentally encounter content not appropriate to their age and interests.

Set time limits – it is recommended that children do not spend more than 1 to 2 hours in front of a computer screen on a daily basis. For children up to 7 years of age, it is best to browse through the contents with them, while for older children, it is important to determine which websites they may and which they may not visit while connected to the internet, before they actually start Internet activities.

Teach your children on safe and responsible online behavior

• Tell your children that they must not share their personal information with strangers on the Internet and remind them that they should use the privacy settings on their personal pages on social networks. The information they post of them should be private or with restricted access. It is sufficient that such information is visible only to their friends and family. They wouldn’t like to display information that might get in the way of enrolling in faculty they want to study at or in the way of getting hired for the job they want. Remind them that revealing personal information about their friends and family isn’t ethical. When posting photos, they need to set them private and not to set tags (tags that describe attendees pictured).

• Children should remember that their passwords are for their own eyes only, and they need to be careful never to enable the option to automatically remember your username and password when checking email or using chat programs from a public computer.

• Teach your children not to meet in person with people they have met online. If you agree your child to meet with one of his cyber friends, it is best to go with him/her and to set the meeting in a public place. Teenagers who probably won’t want to go with an adult, should be accompanied with at least one of their friends.

• Children tend to behave more indecently when online than in person. This behavior triggers the ability to use nicknames that conceal the true culprits of a bad message, and these messages can be easily and quickly spread to all the children in the school. This phenomenon is known as cyberbullying.

• One rule children must obey: if you don’t intend to tell something to someone in person, then don’t tell it by e-mail, SMS, chat and instant message or by posting it to someone's page.

• To protect themselves from unwanted, offensive or intimidating e-mails point out to them that they can use the option to filter unwanted e-mails via the service that have enabled their e-mail address. You can find more information about blocking e-mails from unwanted senders on the link:

http://www.bezbednonainternet.org.mk/blokiranje or http://bezbednonainternet.org.mk/component/option,com_docman/task,doc_download/gid,66/Itemid,38/lang,mk/

• Teach children to share their content responsibly. They need to look up the terms of service before they decide to post something. Also, if they notice any inappropriate content, and if there is an option, they should label it as such to prevent other children from encountering it. This option is available on services like YouTube, which allows setting flags for inappropriate videos, after which they can be deleted.

• Remind your children that everything posted on the Internet, does not necessarily mean it is true. The contents should be viewed critically, the information should be checked from multiple sources as and also they should check the author of the article which they plan to base their school project on or other personal activity of theirs. Teach them how to distinguish reliable from unreliable content and remind them that copying text from a website may constitute plagiarism.

• It may be a good idea to routinely check the history of the computer and your children's phones and ask them to tell you all the passwords for all of their accounts, of course in accordance with the bon ton rules ... But bear in mind that violations of the right to privacy might send distance your child away from you.

• Trust your child enough and don't violate his/her privacy without justified reason.

• Establish boundaries, rules and guidelines of behavior that are allowed on social media and the time allowed to spend on social media. Psychologists warn that teenagers with smart phones/electronic devices tend to be more interested in the cyber world and oblivious to the real world around them, but as a parent you can set rules to prevent it.

• Keep yourself informed about potential threats on the Internet. The dangers of the Internet are much more than just online predators and identity thefts. In fact, teenagers are not the only vulnerable Internet users.

• Even parents can make mistakes on social media!!! Never announce upcoming vacation, and wait until you return home to post photos of the most beautiful beach this summer!

• THE MORE INCLUDED YOU ARE IN THE CYBER WORLD THE MORE YOU'D KNOW ABOUT YOUR CHILD AND HOW TO TALK TO HIM/HER. THE MAIN MESSAGE IS: BE INCLUDED!

Resources:

- www.privacy.mk
- www.metamorphosis.org.mk
- www.bezbednonainternetorg.mk
- www.nemrazi.mk

Appendixes

Appendix 1 - Frequently used acronyms of teenagers

1. **143** I love you
2. **2DAY** Today
3. **4EAE** For ever and ever
4. **ADN** Any day now
5. **AFAIK** As far as I know
6. **AFK** Away from keyboard
7. **ATM** At the moment
8. **B/C** Because
9. **B4** Before
10. **BF / GF** Boyfriend / Girlfriend
11. **BFN** Bye for now
12. **BOL** Be on later
13. **BRB** Be right back
14. **BTW** By the way
15. **DM** Direct message
16. **DWBH** Don't worry, be happy
17. **F2F or FTF** Face to face
18. **FB** Facebook
19. **FF** Follow Friday
20. **FTL** For the loss / For the lose
21. **FTW** For the win
22. **FWB** Friends with benefits
23. **FWIW** For what it's worth
24. **FYEO** For your eyes only
25. **FYI** For your information
26. **GLHF** Good luck, have fun
27. **GR8** Great
28. **HAK** Hugs and kisses
29. **HAND** Have a nice day

30. **HT or H/T** Hat tip or heard through
31. **HTH** Hope this helps / Happy to help
32. **IANAL** I am not a lawyer
33. **IDK** I don’t know
34. **IIRC** If I remember correctly
35. **IKR** I know, right?
36. **ILY / ILU** I love you
37. **IMHO** In my honest opinion / In my humble opinion
38. **IMO** In my opinion
39. **IRL** In real life
40. **IU2U** It’s up to you
41. **IYKWIM** If you know what I mean
42. **J/K** Just kidding
43. **J4F** Just for fun
44. **JIC** Just in case
45. **JSYK** Just so you know
46. **K or KK** Okay
47. **LMBO** Laughing my butt off
48. **LMK** Let me know
49. **LOL** Laughing out loud
50. **MM** Music Monday
51. **MSM** Mainstream media
52. **NAGI** Not a good idea
53. **NM** Never mind
54. **NMU** Not much, you?
55. **NP** No problem or Now playing
56. **NSFW** Not safe for work
57. **NSFL** Not safe for life
58. **NTS** Note to self
59. **OH** Overheard
60. **OMG** Oh my God
61. **ORLY** Oh, really?
62. **PAW** Parents are watching
63. **PLS or PLZ** Please

64. **PPL** People

65. **PTB** Please text back

66. **QQ** Crying.

67. **RAK** Random act of kindness

68. **RL** Real life

69. **ROFL** Rolling on the floor laughing

70. **RT** Retweet

71. **RUOK** Are you okay?

72. **SMH** Shaking my head

73. **SRSLY** Seriously

74. **SSDD** Same stuff, different day

75. **SWAK** Sealed with a kiss

76. **SWYP** So, what’s your problem?

77. **TIA** Thanks in advance

78. **TIME** Tears in my eyes

79. **TMB** Tweet me back

80. **TMI** Too much information

81. **TMRW** Tomorrow

82. **TTYL** Talk to you later

83. **TY or TU** Thank you

84. **VSF** Very sad face

85. **WB** Welcome back

86. **WTH** What the heck?

87. **WTPA** Where the party at?

88. **WYCM** Will you call me?

89. **YGM** You’ve got mail

90. **YMMV** Your mileage may vary

91. **YW** You’re welcome

92. **OMG** Oh my god

CIP – Cataloguing in Publication
National and University Library “St. Climent Ohridski”, Skopje.

004.738.5:342.738-053.5(036)

PARENTS’ guide to protecting children's privacy and personal data
on the internet [Electronic Source] / [Liljana Pecova Ilieska,
Tamara Resavska]. – Text in PDF format contains 34 p... - Skopje
: Metamorfozis : Directorate for personal data protection, 2015

Access method (URL): https://metamorphosis.org.mk
Access method (URL): https://privacy.mk. – Title taken from screen. – Description of the source on day 22.12.2015

ISBN 978-608-4564-59-1 (Metamorphosis)
ISBN 978-608-4682-23-3 (Directorate for Personal Data Protection)

a) Internet – Personal data protection – Guides
COBISS.MK-ID 100210442

[i]

[i] Cover Illustration used under Creative Commons: Bernard Goldbach https://www.flickr.com/photos/topgold